

ỦY BAN NHÂN DÂN THÀNH PHỐ ĐÀ NẴNG

ĐỀ ÁN
THÚC ĐẨY ỨNG DỤNG VÀ PHÁT TRIỂN CÔNG NGHỆ
CHUỖI KHỐI TẠI THÀNH PHỐ ĐÀ NẴNG ĐẾN NĂM 2030

Đà Nẵng, năm 2026

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT VÀ THUẬT NGỮ	6
CHƯƠNG I: BỐI CẢNH XÂY DỰNG ĐỀ ÁN	14
I. CĂN CỨ PHÁP LÝ	14
1. Căn cứ của Trung ương	14
2. Căn cứ của thành phố Đà Nẵng	17
II. SỰ CẦN THIẾT BAN HÀNH ĐỀ ÁN	18
1. Bối cảnh phát triển mới và yêu cầu đặt ra đối với thành phố	18
2. Vị trí của công nghệ blockchain trong hệ thống chính sách	18
3. Bối cảnh phát triển Trung tâm tài chính quốc tế Việt Nam	19
4. Một số tồn tại, hạn chế trong triển khai hiện nay	19
5. Điều kiện và tiền đề của thành phố	20
6. Sự cần thiết ban hành Đề án	20
CHƯƠNG II: HIỆN TRẠNG, XU HƯỚNG VÀ KINH NGHIỆM ỨNG DỤNG BLOCKCHAIN	21
I. HIỆN TRẠNG VÀ KINH NGHIỆM QUỐC TẾ	21
1. Kinh nghiệm ứng dụng blockchain trong dữ liệu tin cậy và dịch vụ công	21
2. Kinh nghiệm về tài chính số, TSMH và hệ sinh thái	23
3. Rủi ro và bài học kinh nghiệm từ thực tiễn quốc tế	26
II. HIỆN TRẠNG VÀ XU HƯỚNG TẠI VIỆT NAM	27
1. Bối cảnh pháp lý, dữ liệu và yêu cầu liên thông	27
2. Xu hướng phát triển hạ tầng blockchain và mô hình dùng chung	28
3. Xu hướng tài chính số, TSMH và sandbox tại Việt Nam	28
III. HIỆN TRẠNG VÀ MỨC ĐỘ SẴN SÀNG CỦA ĐÀ NẴNG	29
1. Điều kiện thể chế và cơ chế triển khai	29
2. Hạ tầng số, dữ liệu và nền tảng tích hợp dùng chung	30
3. Hệ sinh thái doanh nghiệp, cơ sở đào tạo, tổ chức hỗ trợ	31
4. Hiện trạng nguồn nhân lực và năng lực tổ chức thực hiện	31
5. Hiện trạng ứng dụng và thử nghiệm	32
6. Đánh giá tổng hợp mức độ sẵn sàng	32
IV. NHÓM BÀI TOÁN CẦN GIẢI QUYẾT	33
1. Nhóm bài toán về dữ liệu tin cậy, xác minh, toàn vẹn và truy vết trong quản lý nhà nước	33
2. Nhóm bài toán về ứng dụng chuyên ngành có dữ liệu phức tạp, nhạy cảm và điều kiện cao	34
3. Nhóm bài toán về kinh tế dữ liệu và dịch vụ số	34
4. Nhóm bài toán về mô hình chuyên biệt gắn với tài chính số, TSMH, IFC và sandbox	34
CHƯƠNG III: QUAN ĐIỂM, MỤC TIÊU VÀ NỘI DUNG ĐỀ ÁN	35
I. QUAN ĐIỂM XÂY DỰNG ĐỀ ÁN	35

1. Ứng dụng blockchain phục vụ người dân, doanh nghiệp; phát triển chính quyền số và kinh tế dữ liệu	35
2. Bám sát bài toán thực tiễn, phù hợp với mức độ sẵn sàng và khả năng tổ chức thực hiện của thành phố	35
3. Xây dựng hạ tầng chuỗi khối dùng chung của thành phố	35
4. Kết hợp mục tiêu quản lý nhà nước với phát triển hệ sinh thái, huy động sự tham gia của khu vực tư nhân; áp dụng cơ chế đặc thù của thành phố phù hợp phạm vi thẩm quyền	35
5. Gắn với định hướng công nghệ chiến lược quốc gia; tuân thủ pháp luật Việt Nam và tiêu chuẩn kỹ thuật quốc tế, trong nước	36
6. Bảo đảm ATTT, ANM, BVDLCN và quản trị rủi ro xuyên suốt vòng đời	36
7. Phát triển đồng bộ nguồn nhân lực, hệ sinh thái và đổi mới sáng tạo	36
II. NGUYÊN TẮC TRIỂN KHAI	36
1. Dữ liệu nghiệp vụ được quản lý tại hệ thống nguồn; blockchain chỉ ghi nhận lớp tin cậy số cần thiết	36
2. Triển khai theo kiến trúc thống nhất, tích hợp và liên thông có kiểm soát	36
3. Triển khai theo cấp độ, gắn với điều kiện và phạm vi thẩm quyền	37
4. Bảo đảm tuân thủ pháp luật, an toàn, an ninh, bảo vệ dữ liệu và quản trị rủi ro trong toàn bộ quá trình triển khai	37
5. Phân loại nội dung quản lý nhà nước, nội dung doanh nghiệp tham gia và nội dung thực hiện theo cơ chế riêng	38
III. MỤC TIÊU CỦA ĐỀ ÁN	38
1. Mục tiêu tổng quát	38
2. Mục tiêu cụ thể đến năm 2030	38
IV. MÔ HÌNH MẠNG BLOCKCHAIN ĐÀ NẴNG	40
1. Mô hình mạng blockchain trong khung kiến trúc số thành phố	40
2. Kiến trúc DNC-Chain khi tích hợp vào các hệ thống nguồn hiện có	42
3. Mô hình triển khai ứng dụng trên DNC-Chain	43
V. NỘI DUNG TRIỂN KHAI ĐỀ ÁN	45
1. Hoàn thiện thể chế, quản trị và tiêu chuẩn triển khai	45
2. Xây dựng, tổ chức và vận hành hạ tầng DNC-Chain	45
3. Triển khai sản phẩm, ứng dụng	46
4. Chuẩn hóa dữ liệu, tích hợp hệ thống, bảo đảm an toàn và an ninh	47
5. Nguồn nhân lực, hệ sinh thái và đổi mới sáng tạo	48
CHƯƠNG IV: NHIỆM VỤ VÀ GIẢI PHÁP THỰC HIỆN	49
I. VỀ THỂ CHẾ VÀ KHUNG PHÁP LÝ	49
1. Rà soát, hệ thống hoá các văn bản pháp lý	49
2. Ban hành Quy chế quản trị, vận hành và khai thác DNC-Chain	49
3. Ban hành tiêu chuẩn, yêu cầu kết nối, chia sẻ và kiểm chứng dữ liệu	50
4. Ban hành Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án	51

5. Ban hành Quy chế bảo đảm ATTT, ANM và BVDLCN cho DNC-Chain	51
II. VỀ XÂY DỰNG HẠ TẦNG DNC-CHAIN	52
1. Tổ chức triển khai hạ tầng DNC-Chain	52
2. Lựa chọn nền tảng công nghệ Layer-1 của DNC-Chain	52
3. Tổ chức mô hình kiến trúc mạng, node	53
4. Xây dựng các mô đun nền tảng dùng chung của DNC-Chain	55
5. Kết nối DNC-Chain với nền tảng tích hợp và các hệ thống nguồn	58
6. Giám sát, duy trì hoạt động ổn định, dự phòng và ứng cứu sự cố	60
III. VỀ TRIỂN KHAI 10 SẢN PHẨM THEO 04 TẦNG CẤP ĐỘ	60
1. Tầng 1 (SP1, SP2)	60
2. Tầng 2 (SP3, SP4)	63
3. Tầng 3 (SP5, SP6, SP7)	67
4. Tầng 4 (SP8, SP9, SP10)	71
IV. VỀ CHUẨN HÓA DỮ LIỆU, TÍCH HỢP, AN TOÀN THÔNG TIN, AN NINH MẠNG	77
1. Chuẩn hoá dữ liệu và xác định phạm vi dữ liệu đưa vào sử dụng	77
2. Bảo đảm chất lượng, đối soát và xử lý sai lệch dữ liệu trong tích hợp	77
3. Bảo đảm ATTT, ANM và BVDLCN	78
4. Tổ chức kiểm tra, đánh giá, kiểm soát tuân thủ trong quá trình vận hành	78
V. PHÁT TRIỂN NGUỒN NHÂN LỰC VÀ HỆ SINH THÁI	79
1. Đào tạo, bồi dưỡng nguồn nhân lực blockchain	79
2. Ban hành và tổ chức áp dụng Khung năng lực vận hành hệ thống blockchain thành phố	80
3. Phát triển hệ sinh thái doanh nghiệp, viện nghiên cứu và cơ sở đào tạo	80
4. Ban hành và triển khai Kế hoạch thành phố là khách hàng đầu tiên đối với hạ tầng DNC-Chain và sản phẩm blockchain theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ	81
5. Tổ chức đặt hàng nhiệm vụ nghiên cứu, phát triển ứng dụng blockchain cấp thành phố	81
6. Phối hợp với Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai ngay	82
7. Hợp tác quốc tế và chuyển giao công nghệ	82
CHƯƠNG V: TỔ CHỨC THỰC HIỆN	84
I. TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC	84
1. Sở Khoa học và Công nghệ	84
2. Sở Tài chính	86
3. Văn phòng Ủy ban nhân dân thành phố	86
4. Sở Giáo dục và Đào tạo	87
5. Sở Y tế	87
6. Sở Công Thương	87
7. Sở Xây dựng	87

8. Sở Nông nghiệp và Môi trường	88
9. Sở Văn hoá, Thể thao và Du lịch	88
10. Sở Tư pháp	88
11. Sở Nội vụ	88
12. Sở Ngoại vụ	89
13. Công an thành phố Đà Nẵng	89
14. Cơ quan điều hành Trung tâm tài chính quốc tế Việt Nam tại Đà Nẵng	90
15. Ngân hàng Nhà nước khu vực 9	90
16. Các sở, ban, ngành và Ủy ban nhân dân các phường, xã, đặc khu	90
17. Doanh nghiệp cung cấp công nghệ và hạ tầng kỹ thuật	91
18. Doanh nghiệp, tổ chức tham gia cơ chế sandbox	91
19. Các cơ sở đào tạo, viện nghiên cứu	92
20. Các tổ chức đoàn thể và cơ quan truyền thông, báo chí	92
II. CƠ CHẾ PHỐI HỢP LIÊN NGÀNH VÀ XỬ LÝ VƯỚNG MẮC	92
1. Cơ chế phối hợp liên ngành	92
2. Xử lý vướng mắc trong quá trình thực hiện	93
III. KẾ HOẠCH TRIỂN KHAI ĐỀ ÁN	93
IV. NGUỒN LỰC TÀI CHÍNH VÀ PHÂN BỐ NGUỒN LỰC	94
1. Nguyên tắc bố trí và sử dụng nguồn lực	94
2. Phân định nguồn lực theo tính chất đầu tư	94
3. Cơ cấu phân bổ nguồn lực theo nhóm nhiệm vụ và tầng cấp độ	96
4. Tổng nhu cầu kinh phí thực hiện Đề án	98
CHƯƠNG VI: HIỆU QUẢ DỰ KIẾN, CHỈ TIÊU ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO	100
I. HIỆU QUẢ DỰ KIẾN	100
1. Hiệu quả đối với quản lý nhà nước và dịch vụ công	100
2. Hiệu quả đối với hạ tầng số, dữ liệu và năng lực tích hợp	100
3. Hiệu quả đối với kinh tế số, đổi mới sáng tạo và hệ sinh thái	101
4. Hiệu quả đối với năng lực tổ chức thực hiện của thành phố	101
5. Hiệu quả tổng thể đối với phát triển kinh tế - xã hội và đóng góp vào mục tiêu quốc gia	102
II. HỆ THỐNG CHỈ TIÊU ĐÁNH GIÁ	102
1. Nguyên tắc xây dựng và áp dụng chỉ tiêu	102
2. Hệ chỉ tiêu tổng hợp cấp Đề án	103
3. Hệ chỉ tiêu theo sản phẩm trọng điểm	106
4. Sử dụng kết quả đo lường chỉ tiêu	108
III. CƠ CHẾ ĐÁNH GIÁ KẾT QUẢ THỰC HIỆN	108
1. Nguyên tắc đánh giá	108
2. Cơ quan chủ trì và trách nhiệm phối hợp	108
3. Phương pháp đánh giá	109

4. Thời điểm và chu kỳ đánh giá	109
IV. QUẢN LÝ RỦI RO VÀ ĐIỀU CHỈNH ĐỀ ÁN	110
1. Nguyên tắc quản lý rủi ro	110
2. Các nhóm rủi ro chính và biện pháp xử lý	110
3. Cơ chế điều chỉnh Đề án	112
Phụ lục I	1
THUYẾT MINH KỸ THUẬT NỀN TẢNG DNC-CHAIN, CÁC MÔ ĐUN NỀN TẢNG DÙNG CHUNG VÀ SẢN PHẨM ỨNG DỤNG	1
Phụ lục II	1
DỰ TOÁN KINH PHÍ	1
Phụ lục III	1
DANH MỤC NHIỆM VỤ, CHƯƠNG TRÌNH, DỰ ÁN, SẢN PHẨM, HẠNG MỤC ĐẦU TƯ	1
VÀ ĐẦU MỐI CHỦ TRÌ	1

DANH MỤC TỪ VIẾT TẮT VÀ THUẬT NGỮ

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
1	ACL	Access Control List - Danh sách kiểm soát truy cập
2	AccessGate	Cổng kiểm soát truy cập cấp ứng dụng trên DNC-Chain
3	AES	Advanced Encryption Standard - Chuẩn mã hoá tiên tiến
4	AML	Anti-Money Laundering - Phòng, chống rửa tiền
5	AML/CFT/CTTPBV KHDHL	Phòng, chống rửa tiền/Chống tài trợ khủng bố/Chống tài trợ phổ biến vũ khí hủy diệt hàng loạt
6	ANM	An ninh mạng
7	API	Application Programming Interface - Giao diện lập trình ứng dụng
8	Attestation	Chứng thực khối trong cơ chế đồng thuận PoS
9	ATTT	An toàn thông tin mạng
10	Batching	Gom lô bằng chứng để tối ưu chi phí ghi nhận lên chuỗi
11	BCA	Bộ Công an
12	BCM	Business Continuity Management - Quản lý liên tục hoạt động
13	BGDĐT	Bộ Giáo dục và Đào tạo
14	BIM	Building Information Modeling - Mô hình thông tin công trình
15	BKHCN	Bộ Khoa học và Công nghệ
16	BLS	Boneh-Lynn-Shacham - Lược đồ chữ ký số nhóm dùng trong tổng hợp chữ ký
17	BSN	Blockchain-based Service Network - Mạng dịch vụ blockchain dùng chung quốc gia (Trung Quốc)
18	BTC	Bộ Tài chính (trong ngữ cảnh cơ quan Việt Nam); Bitcoin (trong ngữ cảnh tài sản mã hoá)
19	BVDLCN	Bảo vệ dữ liệu cá nhân
20	CCCD	Căn cước công dân
21	CDS	Chuyển đổi số
22	CFT	Combating the Financing of Terrorism - Chống tài trợ khủng bố
23	CityGML	City Geography Markup Language - Chuẩn mô hình thông tin

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
		đô thị 3D
24	Compliance Layer	Lớp tuân thủ tự động thực thi quy tắc tại hợp đồng thông minh
25	ConsentGranted	Trạng thái cấp quyền đồng ý của chủ thể dữ liệu
26	ConversionGateway	Cổng chuyển đổi có kiểm soát giữa các loại token
27	Cosmos SDK	Bộ công cụ phát triển blockchain chuyên đề trong hệ sinh thái Cosmos
28	CosmWasm	Máy ảo hợp đồng thông minh dựa trên WebAssembly cho Cosmos
29	CP	Chính phủ
30	CRL	Certificate Revocation List - Danh sách thu hồi chứng thư số
31	Cross-Chain Messaging	Truyền thông điệp liên chuỗi
32	CRYSTALS	Cryptographic Suite for Algebraic Lattices - Bộ thuật toán mật mã hậu lượng tử (gồm Kyber, Dilithium)
33	CSDL	Cơ sở dữ liệu
34	CSDLQG	Cơ sở dữ liệu quốc gia
35	CTTPBVKHDHL	Chống tài trợ phổ biến vũ khí huỷ diệt hàng loạt
36	CV	Công văn
37	DFSA	Dubai Financial Services Authority - Cơ quan Dịch vụ tài chính Dubai
38	DID	Decentralized Identifier - Định danh phi tập trung (chuẩn W3C)
39	DIFC	Dubai International Financial Centre - Trung tâm tài chính quốc tế Dubai
40	DLT	Distributed Ledger Technology - Công nghệ sổ cái phân tán
41	DNC-Chain	Da Nang City Chain - Hạ tầng chuỗi khối dùng chung của thành phố Đà Nẵng
42	ĐMST	Đổi mới sáng tạo
43	EBSI	European Blockchain Services Infrastructure - Hạ tầng dịch vụ blockchain châu Âu
44	ECDSA	Elliptic Curve Digital Signature Algorithm - Thuật toán chữ ký số đường cong elliptic

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
45	EIP	Ethereum Improvement Proposal - Đề xuất cải tiến Ethereum
46	ERC	Ethereum Request for Comments - Chuẩn token và giao thức trên Ethereum
47	Ethermint	Mô đun tương thích EVM trên Cosmos SDK
48	EU	European Union - Liên minh châu Âu
49	EVM	Ethereum Virtual Machine - Máy ảo Ethereum
50	Expiry	Thời hạn hiệu lực của token, chứng nhận
51	FATF	Financial Action Task Force - Lực lượng đặc nhiệm tài chính (về phòng, chống rửa tiền)
52	FFG	Friendly Finality Gadget - Cơ chế hoàn tất khối Casper trong Ethereum PoS
53	FHIR	Fast Healthcare Interoperability Resources - Chuẩn liên thông dữ liệu y tế
54	Finalization	Hoàn tất khối
55	FIPS	Federal Information Processing Standards - Tiêu chuẩn xử lý thông tin liên bang (Hoa Kỳ)
56	FISCO BCOS	Financial Services Industry Consortium - Blockchain Open Source - Nền tảng blockchain mã nguồn mở do liên minh tài chính Trung Quốc phát triển
57	FPT	Tập đoàn FPT
58	FSB	Financial Stability Board - Ủy ban Ổn định Tài chính
59	FTX	Sàn giao dịch tài sản mã hoá FTX (đã phá sản năm 2022)
60	GDP	Gross Domestic Product - Tổng sản phẩm quốc nội
61	GDPR	General Data Protection Regulation - Quy định bảo vệ dữ liệu chung của Liên minh châu Âu
62	Governance	Token quản trị; chức năng quản trị on-chain
63	GPS	Global Positioning System - Hệ thống định vị toàn cầu
64	GRDP	Gross Regional Domestic Product - Tổng sản phẩm trên địa bàn
65	gRPC	gRPC Remote Procedure Call - Giao thức gọi thủ tục từ xa hiệu năng cao của Google

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
66	Hash	Giá trị băm mật mã
67	HĐND	Hội đồng nhân dân
68	HIS	Hospital Information System - Hệ thống thông tin bệnh viện
69	HKD	Hong Kong Dollar - Đô la Hồng Kông
70	HSM	Hardware Security Module - Mô đun bảo mật phần cứng
71	HTTPS	Hypertext Transfer Protocol Secure - Giao thức truyền siêu văn bản bảo mật
72	Hub ID	Mã định danh kỹ thuật vô danh do Mô đun 7 cấp phát trên DNC-Chain
73	Hyperledger Besu	Nền tảng blockchain doanh nghiệp tương thích EVM của Hyperledger
74	Hyperledger Fabric	Nền tảng blockchain có cấp phép modular của Hyperledger
75	IBC	Inter-Blockchain Communication - Giao thức liên thông giữa các blockchain trong Cosmos
76	IBFT	Istanbul Byzantine Fault Tolerant - Cơ chế đồng thuận Istanbul
77	IBM	International Business Machines Corporation
78	ICD	International Classification of Diseases - Phân loại bệnh tật quốc tế
79	IEC	International Electrotechnical Commission - Ủy ban Kỹ thuật điện quốc tế
80	IFC	International Financial Center - Trung tâm tài chính quốc tế; cũng là Industry Foundation Classes - chuẩn dữ liệu BIM (theo ngữ cảnh)
81	ISO	International Organization for Standardization - Tổ chức Tiêu chuẩn hóa quốc tế
82	JWT	JSON Web Token - Chuẩn token xác thực dạng JSON
83	KH&CN	Khoa học và Công nghệ
84	KMS	Key Management Service - Dịch vụ quản lý khoá mật mã
85	KSI	Keyless Signature Infrastructure - Hạ tầng chữ ký không khoá
86	KYC	Know Your Customer - Nhận biết khách hàng

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
87	Layer-1	Lớp hạ tầng nền của blockchain
88	LGSP	Local Government Service Platform - Nền tảng tích hợp, chia sẻ dữ liệu cấp tỉnh, thành phố
89	LicenseSBT	Token định danh giấy phép dạng Soulbound
90	Loyalty	Token điểm thưởng
91	MAS	Monetary Authority of Singapore - Cơ quan Quản lý Tiền tệ Singapore
92	Merkle Proof	Bằng chứng Merkle - cơ chế chứng minh thành viên trong cây băm Merkle
93	mTLS	Mutual Transport Layer Security - Xác thực TLS hai chiều
94	NĐ	Nghị định
95	NIST	National Institute of Standards and Technology - Viện Tiêu chuẩn và Công nghệ Hoa Kỳ
96	Node	Nút mạng tham gia blockchain (validator node, admin node, service node)
97	NQ	Nghị quyết
98	NSNN	Ngân sách nhà nước
99	OAuth	Open Authorization - Chuẩn ủy quyền mở (OAuth 2.0)
100	OECD	Organisation for Economic Co-operation and Development - Tổ chức Hợp tác và Phát triển Kinh tế
101	OGC	Open Geospatial Consortium - Liên minh chuẩn không gian địa lý mở
102	OIDC	OpenID Connect - Chuẩn kết nối định danh mở
103	OIDC4VCI	OpenID Connect for Verifiable Credential Issuance - Chuẩn OIDC cho phát hành Chứng nhận xác minh
104	OIDC4VP	OpenID Connect for Verifiable Presentations - Chuẩn OIDC cho trình bày, xác minh Chứng nhận xác minh
105	On-chain / Off-chain	Trên chuỗi / Ngoài chuỗi
106	Optimistic Rollup	Giải pháp mở rộng Layer-2 dựa trên giả định lạc quan
107	OTP	One-Time Password - Mật khẩu một lần
108	Permissioned	Có cấp phép (đối với mạng blockchain)

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
109	PKCE	Proof Key for Code Exchange - Cơ chế bảo vệ trao đổi mã của OAuth 2.0
110	PKCS	Public-Key Cryptography Standards - Chuẩn mật mã khoá công khai (PKCS#11)
111	PLONK	Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge - Lược đồ chứng minh không tiết lộ tri thức
112	PoA	Proof of Authority - Cơ chế đồng thuận chứng nhận thẩm quyền
113	PoS	Proof of Stake - Cơ chế đồng thuận chứng minh cổ phần
114	Proxy Upgrade Pattern	Mẫu thiết kế hợp đồng thông minh có thể nâng cấp qua proxy
115	QBFT	Quorum Byzantine Fault Tolerant - Cơ chế đồng thuận Quorum
116	QCVN	Quy chuẩn kỹ thuật quốc gia
117	QĐ	Quyết định
118	QH	Quốc hội
119	RBAC	Role-Based Access Control - Kiểm soát truy cập dựa trên vai trò
120	REST	Representational State Transfer - Kiến trúc giao tiếp dịch vụ web
121	Revocation	Thu hồi (bằng chứng, chứng nhận, token)
122	RFC	Request for Comments - Tài liệu chuẩn kỹ thuật Internet
123	Rollup	Giải pháp mở rộng blockchain Layer-2 (Optimistic Rollup, ZK-Rollup)
124	RPC	Remote Procedure Call - Lệnh gọi thủ tục từ xa
125	RPO	Recovery Point Objective - Mất dữ liệu tối đa cho phép
126	RTO	Recovery Time Objective - Thời gian phục hồi sau sự cố
127	RWA	Real-World Assets - Tài sản thực được token hoá
128	Sandbox	Cơ chế thử nghiệm có kiểm soát
129	SBT	Soulbound Token - Token không thể chuyển nhượng

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
130	SDK	Software Development Kit - Bộ công cụ phát triển phần mềm
131	Self-Sovereign Identity	Định danh tự chủ
132	SHA	Secure Hash Algorithm - Thuật toán băm bảo mật (SHA-256, SHA-3)
133	Smart contract	Hợp đồng thông minh
134	SP1 - SP11	Sản phẩm số 1 đến Sản phẩm số 11 trong danh mục sản phẩm ứng dụng của Đề án
135	Sovereignty	Tính chủ quyền của mạng blockchain
136	Stablecoin	Tài sản mã hoá ổn định giá, neo theo tiền pháp định hoặc tài sản tham chiếu
137	TB	Thông báo
138	TCVN	Tiêu chuẩn quốc gia Việt Nam
139	Time-lock	Quy tắc tuân thủ ở Compliance Layer (Mô đun 4) – khoá chuyển nhượng/giao dịch token cho đến mốc thời gian quy định
140	Timelock	Cơ chế quản trị nâng cấp - thời gian chờ bắt buộc (mặc định 48 giờ) giữa khi đa ký phê duyệt và khi thực thi nâng cấp hợp đồng, đổi validator, whitelist
141	TLS	Transport Layer Security - Bảo mật tầng truyền tải
142	Token hoá	Tokenization - Mã hoá tài sản hoặc quyền sở hữu dưới dạng token trên blockchain
143	TPS	Transactions Per Second - Số giao dịch xử lý mỗi giây
144	Travel Rule	Quy tắc Travel Rule của FATF về cung cấp thông tin người gửi, người nhận trong giao dịch TSMH
145	TSMH	Tài sản mã hoá
146	TT	Thông tư
147	TTDL	Trung tâm dữ liệu
148	TTg	Thủ tướng Chính phủ
149	TW	Trung ương
150	UBND	Ủy ban nhân dân

STT	Viết tắt / Thuật ngữ	Tên đầy đủ / Nghĩa
151	USD	United States Dollar - Đô la Mỹ
152	USDT	Tether USD - Stablecoin neo USD do Tether phát hành
153	UUPS	Universal Upgradeable Proxy Standard - Chuẩn proxy nâng cấp đa dụng (EIP-1822)
154	Validator	Trình xác thực - Nút tham gia tạo và xác minh khối trong cơ chế đồng thuận PoS
155	Validium	Giải pháp mở rộng Layer-2 lưu trữ dữ liệu ngoài chuỗi kết hợp ZK Proof
156	VARA	Virtual Assets Regulatory Authority - Cơ quan Quản lý Tài sản ảo Dubai
157	VBA	Vietnam Blockchain Association - Hiệp hội Blockchain và Tài sản số Việt Nam
158	VBQPPL	Văn bản quy phạm pháp luật
159	VBSN	Vietnam Blockchain Service Network - Mạng dịch vụ blockchain đa chuỗi Việt Nam
160	VC	Verifiable Credential - Chứng nhận xác minh (chuẩn W3C)
161	Verification	Kiểm chứng bằng chứng
162	VNeID	Ứng dụng định danh điện tử quốc gia Việt Nam
163	VND	Đồng Việt Nam
164	VNPT	Tập đoàn Bưu chính Viễn thông Việt Nam
165	VRF	Verifiable Random Function - Hàm ngẫu nhiên có thể xác minh
166	W3C	World Wide Web Consortium - Liên minh Web toàn cầu
167	WIPO	World Intellectual Property Organization - Tổ chức Sở hữu trí tuệ thế giới
168	ZK	Zero-Knowledge - Không tiết lộ tri thức
169	ZKP	Zero-Knowledge Proof - Bằng chứng không tiết lộ tri thức
170	ZK-Rollup	Giải pháp mở rộng Layer-2 dựa trên bằng chứng không tiết lộ tri thức

CHƯƠNG I: BỐI CẢNH XÂY DỰNG ĐỀ ÁN

I. CĂN CỨ PHÁP LÝ

1. Căn cứ của Trung ương

Đề án được xây dựng trên cơ sở các chủ trương, đường lối của Đảng và chính sách, pháp luật của Nhà nước về phát triển khoa học và công nghệ (KH&CN), đổi mới sáng tạo (ĐMST) và chuyển đổi số (CDS); về dữ liệu, giao dịch điện tử, bảo vệ dữ liệu cá nhân (BVDLCN), an toàn thông tin mạng (ATTT), an ninh mạng (ANM), Chính phủ số và nền tảng số dùng chung; về công nghệ chiến lược, công nghệ chuỗi khối (blockchain), Trung tâm tài chính quốc tế (IFC) Việt Nam đặt tại Thành phố Hồ Chí Minh và thành phố Đà Nẵng và thí điểm thị trường tài sản mã hoá (TSMH) tại Việt Nam.

Các căn cứ của Trung ương tạo cơ sở chính trị, pháp lý để thành phố Đà Nẵng tổ chức triển khai các mô hình ứng dụng blockchain phù hợp với điều kiện thực tiễn của địa phương, tập trung vào các nhóm văn bản chủ yếu sau:

a) Nhóm chủ trương, chính sách nền tảng về khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số

- Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư;

- Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

- Nghị quyết số 03/NQ-CP ngày 09/01/2025 của Chính phủ ban hành Chương trình hành động thực hiện Nghị quyết số 57-NQ/TW;

- Nghị quyết số 71/NQ-CP ngày 01/4/2025 của Chính phủ sửa đổi, bổ sung, cập nhật Chương trình hành động thực hiện Nghị quyết số 57-NQ/TW.

- Công văn số 562/BKHCN-VCL ngày 31/3/2025 của Bộ Khoa học và Công nghệ hướng dẫn làm rõ định nghĩa, nội hàm, lượng hóa một số khái niệm mới trong Nghị quyết số 57-NQ/TW.

b) Nhóm pháp luật về giao dịch điện tử, dữ liệu, bảo vệ dữ liệu cá nhân và sở hữu trí tuệ

- Luật Giao dịch điện tử số 20/2023/QH15 ngày 22/6/2023;

- Luật Dữ liệu số 60/2024/QH15 ngày 30/11/2024;

- Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025;

- Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân (thay thế Nghị định số 13/2023/NĐ-CP ngày 17/4/2023);

- Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015, được sửa đổi, bổ sung bởi Luật số 35/2018/QH14 ngày 12/6/2018;

- Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018 và Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025 của Quốc hội (có hiệu lực thi hành kể từ ngày 01/7/2026, hợp nhất và thay thế Luật An toàn thông tin mạng số 86/2015/QH13 (sửa đổi, bổ sung bởi Luật số 35/2018/QH14) và Luật An ninh mạng số 24/2018/QH14);

- Luật Căn cước số 26/2023/QH15 ngày 27/11/2023;

- Luật Công nghiệp công nghệ số số 71/2025/QH15 ngày 14/6/2025;

- Luật Trí tuệ nhân tạo số 134/2025/QH15 ngày 10/12/2025;

- Luật Chuyển đổi số số 148/2025/QH15 ngày 11/12/2025;

- Luật Sở hữu trí tuệ số 50/2005/QH11 ngày 29/11/2005, được sửa đổi, bổ sung bởi Luật số 36/2009/QH12 ngày 19/6/2009, Luật số 42/2019/QH14 ngày 14/6/2019 và Luật số 07/2022/QH15 ngày 16/6/2022.

c) Nhóm quy định về liên thông, chia sẻ dữ liệu, chuẩn hoá dữ liệu và quản trị dữ liệu

- Nghị định số 278/2025/NĐ-CP ngày 22/10/2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị;

- Nghị định số 165/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu;

- Nghị định số 169/2025/NĐ-CP ngày 30/6/2025 của Chính phủ quy định hoạt động khoa học, công nghệ, đổi mới sáng tạo và sản phẩm, dịch vụ về dữ liệu;

- Nghị định số 102/2025/NĐ-CP ngày 13/5/2025 của Chính phủ quy định quản lý dữ liệu y tế;

- Quy định số 05-QĐ/BCĐTW ngày 27/8/2025 của Ban Chỉ đạo Trung ương về mô hình liên thông số thống nhất, hiệu quả và quản trị dựa trên dữ liệu trong hệ thống chính trị;

- Kế hoạch số 02-KH/BCĐTW ngày 19/6/2025 của Ban Chỉ đạo Trung ương về thúc đẩy chuyển đổi số liên thông, đồng bộ, nhanh, hiệu quả;

- Nghị quyết số 214/NQ-CP ngày 23/7/2025 của Chính phủ ban hành kế hoạch hành động thúc đẩy tạo lập dữ liệu phục vụ chuyển đổi số toàn diện;

- Quyết định số 2439/QĐ-TTg ngày 04/11/2025 của Thủ tướng Chính phủ ban hành Khung kiến trúc dữ liệu quốc gia, Khung quản trị, quản lý dữ liệu quốc gia, Từ điển dữ liệu dùng chung (phiên bản 1.0);

- Quyết định số 20/2025/QĐ-TTg ngày 01/7/2025 về Danh mục dữ liệu quan trọng, dữ liệu cốt lõi;

- Thông tư số 10/2026/TT-BGDĐT ngày 26/02/2026 của Bộ Giáo dục và Đào tạo ban hành Quy chế văn bằng, chứng chỉ của hệ thống giáo dục quốc dân.

d) Nhóm chương trình, đề án và khung kiến trúc về Chính phủ số, nền tảng số dùng chung, hạ tầng số

- Quyết định số 749/QĐ-TTg ngày 03/6/2020 phê duyệt Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030;

- Nghị quyết số 175/NQ-CP ngày 30/10/2023 phê duyệt Đề án Trung tâm dữ liệu quốc gia;

- Quyết định số 2629/QĐ-TTg ngày 01/12/2025 phê duyệt Chương trình phát triển Chính phủ số;

- Quyết định số 292/QĐ-BKHCN ngày 25/3/2025 ban hành Khung kiến trúc Chính phủ số Việt Nam, phiên bản 4.0;

- Quyết định số 3090/QĐ-BKHCN ngày 08/10/2025 ban hành Khung kiến trúc tổng thể quốc gia số;

- Quyết định số 2618/QĐ-BKHCN ngày 11/9/2025 ban hành Danh mục và kế hoạch triển khai các nền tảng số quốc gia, nền tảng số dùng chung của ngành, lĩnh vực, vùng;

- Công văn 7181/BKHCN-TĐC, ngày 29/11/2025 của Bộ Khoa học và Công nghệ, hướng dẫn danh mục tiêu chuẩn, quy chuẩn kỹ thuật (TCVN/QCVN) cho các lĩnh vực công nghệ chiến lược;

- Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

đ) Nhóm định hướng phát triển công nghệ blockchain, công nghệ chiến lược và cơ chế liên quan đến Trung tâm tài chính quốc tế, thị trường tài sản mã hóa

- Nghị quyết số 222/2025/QH15 ngày 27/6/2025 của Quốc hội về IFC tại Việt Nam;

- Quyết định số 1236/QĐ-TTg ngày 22/10/2024 ban hành Chiến lược quốc gia về ứng dụng và phát triển công nghệ blockchain đến năm 2025, định hướng đến năm 2030;

- Quyết định số 1131/QĐ-TTg ngày 12/6/2025 ban hành Danh mục công nghệ chiến lược và sản phẩm công nghệ chiến lược và Quyết định số 21/2026/QĐ-TTg ngày 30/4/2026 của Thủ tướng Chính phủ ban hành Danh mục công nghệ chiến lược và Danh mục sản phẩm công nghệ chiến lược (có hiệu lực thi hành kể từ ngày 01/7/2026, thay thế Quyết định số 1131/QĐ-TTg);

- Quyết định số 2815/QĐ-TTg ngày 28/12/2025 phê duyệt Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai nhanh;

- Thông báo kết luận số 47-TB/TW ngày 15/11/2024 của Bộ Chính trị về xây dựng Trung tâm tài chính khu vực và quốc tế tại Việt Nam;

- Nghị quyết số 259/NQ-CP ngày 31/12/2024 của Chính phủ phê duyệt Kế hoạch hành động triển khai xây dựng Trung tâm tài chính khu vực và quốc tế tại Việt Nam;

- Nghị định số 323/2025/NĐ-CP ngày 18/12/2025 của Chính phủ về thành lập Trung tâm tài chính quốc tế tại Việt Nam;

- Nghị định số 324/2025/NĐ-CP ngày 18/12/2025 của Chính phủ về Chính sách tài chính trong Trung tâm tài chính quốc tế tại Việt Nam;

- Nghị định số 329/2025/NĐ-CP ngày 18/12/2025 của Chính phủ về cấp phép thành lập và hoạt động ngân hàng, quản lý ngoại hối, phòng chống rửa tiền, chống tài trợ khủng bố, chống tài trợ phổ biến vũ khí hủy diệt hàng loạt tại Trung tâm tài chính quốc tế tại Việt Nam;

- Luật Phòng, chống rửa tiền số 14/2022/QH15 ngày 15/11/2022;

- Luật Đầu tư số 143/2025/QH15 ngày 27/6/2025;

- Nghị quyết số 05/2025/NQ-CP ngày 09/9/2025 của Chính phủ về triển khai thí điểm thị trường tài sản mã hóa tại Việt Nam;

- Thông tư số 15/2026/TT-BTC ngày 04/3/2026 của Bộ Tài chính hướng dẫn nguyên tắc kế toán đối với các tổ chức tham gia thị trường tài sản mã hóa tại Việt Nam.

2. Căn cứ của thành phố Đà Nẵng

Đề án đồng thời được xây dựng trên cơ sở các chủ trương, chính sách, cơ chế đặc thù và văn bản điều hành của thành phố về đổi mới sáng tạo, chuyển đổi số, phát triển hạ tầng số, cơ chế sandbox đối với công nghệ mới và xây dựng khung kiến trúc số thành phố. Đây là cơ sở quan trọng để tổ chức triển khai Đề án gắn với định hướng phát triển chính quyền số, kinh tế số, kinh tế dữ liệu và hệ sinh thái đổi mới sáng tạo của thành phố. Các căn cứ chủ yếu của thành phố gồm:

- Nghị quyết số 43-NQ/TW ngày 24/01/2019 của Bộ Chính trị về xây dựng và phát triển thành phố Đà Nẵng đến năm 2030, tầm nhìn đến năm 2045;

- Nghị quyết số 136/2024/QH15 ngày 26/6/2024 của Quốc hội về tổ chức chính quyền đô thị và thí điểm một số cơ chế, chính sách đặc thù phát triển thành phố Đà Nẵng;

- Nghị quyết số 259/2025/QH15 ngày 11/12/2025 của Quốc hội sửa đổi, bổ sung một số điều của Nghị quyết số 136/2024/QH15;

- Nghị quyết Đại hội đại biểu lần thứ I Đảng bộ thành phố Đà Nẵng nhiệm kỳ 2025-2030;

- Nghị quyết số 05-NQ/TU ngày 17/6/2021 của Ban Chấp hành Đảng bộ thành phố Đà Nẵng về chuyển đổi số trên địa bàn thành phố đến năm 2025, định hướng đến năm 2030;

- Kế hoạch hành động số 21-KH/TU ngày 10/9/2025 của Ban Thường vụ Thành ủy Đà Nẵng thực hiện Nghị quyết số 57-NQ/TW;

- Nghị quyết số 55/2024/NQ-HĐND ngày 13/12/2024 của Hội đồng nhân dân thành phố quy định tiêu chí, điều kiện và thủ tục thử nghiệm có kiểm soát các giải pháp công nghệ mới trên địa bàn thành phố;

- Quyết định số 1181/QĐ-UBND ngày 26/8/2025 của Ủy ban nhân dân thành phố Đà Nẵng về việc cấp Giấy chứng nhận thử nghiệm có kiểm soát đối với sản phẩm chuyển đổi tài sản mã hóa sang tiền pháp định;

- Quyết định số 3292/QĐ-UBND ngày 30/12/2025 của Ủy ban nhân dân thành phố Đà Nẵng về việc ban hành Đề án chuyển đổi số góp phần thúc đẩy, tạo động lực phát triển kinh tế - xã hội thành phố giai đoạn 2026-2030, định hướng đến năm 2035;

- Quyết định số 3291/QĐ-UBND ngày 30/12/2025 ban hành Khung kiến trúc số thành phố Đà Nẵng;

- Quyết định số 3405/QĐ-UBND ngày 31/12/2025 ban hành Kiến trúc tổng thể thành phố thông minh thành phố Đà Nẵng, phiên bản 2.0.

- Kế hoạch số 122/KH-UBND ngày 06/10/2025 của Ủy ban nhân dân thành phố Đà Nẵng triển khai Kế hoạch hành động thực hiện Nghị quyết số 57-NQ/TW trên địa bàn thành phố;

Hệ thống các căn cứ nêu trên là cơ sở để thành phố xây dựng Đề án bảo đảm phù hợp với định hướng chiến lược từ Trung ương, khung pháp luật chuyên ngành về dữ liệu, giao dịch điện tử, BVDLCN, ATTT, ANM, hạ tầng số, cơ chế đặc thù của Đà Nẵng và các quy định liên quan đến tài chính số, TSMH, IFC Việt Nam đặt tại Thành phố Hồ Chí Minh và thành phố Đà Nẵng và sandbox.

II. SỰ CẦN THIẾT BAN HÀNH ĐỀ ÁN

1. Bối cảnh phát triển mới và yêu cầu đặt ra đối với thành phố

Giai đoạn 2026-2030, đất nước bước vào chặng phát triển mới với yêu cầu tăng trưởng nhanh và bền vững trên nền tảng KH&CN, ĐMST và CDS. Đại hội đại biểu toàn quốc lần thứ XIV của Đảng xác định KH&CN, ĐMST và CDS là động lực tăng trưởng chủ yếu; kinh tế số, kinh tế dữ liệu, kinh tế xanh và kinh tế tuần hoàn được xác lập như những trụ cột của mô hình phát triển mới.

Đối với thành phố Đà Nẵng, yêu cầu này càng rõ hơn khi thành phố được định hướng trở thành trung tâm khoa học, công nghệ, đổi mới sáng tạo, logistics, tài chính và đô thị hiện đại của khu vực miền Trung; đồng thời được trao cơ chế, chính sách đặc thù để chủ động hơn trong tổ chức phát triển. Do đó, thành phố cần có một khung triển khai thống nhất để lựa chọn đúng nội dung ưu tiên, tổ chức hạ tầng phù hợp, huy động được các chủ thể tham gia và bảo đảm ứng dụng công nghệ mới gắn chặt với yêu cầu phát triển thực tiễn.

2. Vị trí của công nghệ blockchain trong hệ thống chính sách

Blockchain là công nghệ không nhằm thay thế các hệ thống hiện có, mà phát huy giá trị rõ nhất ở vai trò tạo lập lớp tin cậy số phục vụ xác minh, kiểm chứng, truy vết, đối soát và hỗ trợ khai thác dữ liệu tin cậy trong các hoạt động số có nhiều chủ thể tham gia. Trong bối cảnh dữ liệu ngày càng được tạo lập, chia sẻ và xử lý trên quy mô lớn, yêu cầu không chỉ dừng ở số hoá, mà còn mở rộng sang xác minh tính toàn vẹn, làm rõ trách nhiệm xử lý và tăng khả năng kiểm chứng độc lập.

Trong nước, blockchain đã được xác lập trong hệ thống chính sách quốc gia, bao trùm các mặt từ hạ tầng số, dữ liệu tin cậy, đổi mới sáng tạo và phát triển công nghệ chiến lược. Quyết định số 1236/QĐ-TTg ban hành Chiến lược quốc gia về ứng dụng và phát triển công nghệ blockchain đến năm 2025, định hướng đến năm 2030 với các mục

tiêu hình thành hạ tầng blockchain, thúc đẩy ứng dụng trong chính quyền điện tử, phát triển hệ sinh thái và hoàn thiện khung pháp lý. Quyết định số 1131/QĐ-TTg và Quyết định số 21/2026/QĐ-TTg (thay thế Quyết định số 1131/QĐ-TTg kể từ ngày 01/7/2026) đưa blockchain vào Danh mục công nghệ chiến lược của quốc gia, khẳng định blockchain là một trong những công nghệ ưu tiên cho phát triển. Quyết định số 2815/QĐ-TTg phê duyệt Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai nhanh, trong đó có các sản phẩm ứng dụng blockchain.

Trên cơ sở đó, blockchain có ý nghĩa đối với thành phố Đà Nẵng ở các phương diện chính như: hỗ trợ nâng cao độ tin cậy, tính minh bạch và trách nhiệm giải trình trong quản lý nhà nước và dịch vụ công; bổ sung nền tảng kỹ thuật cho các hoạt động khai thác dữ liệu, xác minh giao dịch và phát triển dịch vụ số; tạo điều kiện để thành phố từng bước thu hút doanh nghiệp, phát triển hệ sinh thái, thúc đẩy đổi mới sáng tạo và tham gia vào các mô hình kinh tế số mới. Vì vậy, việc triển khai blockchain tại Đà Nẵng được đặt trong tổng thể định hướng phát triển công nghệ chiến lược của quốc gia và định hướng phát triển kinh tế số của thành phố, đóng vai trò triển khai ở địa bàn và đóng góp thực tiễn vào quá trình phát triển chung.

3. Bối cảnh phát triển Trung tâm tài chính quốc tế Việt Nam

Trên thế giới, blockchain đang được áp dụng làm công nghệ hạ tầng cho các mô hình kinh tế số, tài chính số và kinh tế dữ liệu, đặc biệt trong xác thực giao dịch, lưu vết dữ liệu, hợp đồng thông minh và tài sản thực được token hoá (RWA). Trong nước, việc hình thành IFC Việt Nam đặt tại Thành phố Hồ Chí Minh và thành phố Đà Nẵng theo Nghị quyết số 222/2025/QH15 và Nghị định số 323/2025/NĐ-CP, cùng với khung thí điểm thị trường TSMH theo Nghị quyết số 05/2025/NQ-CP, tạo ra một không gian chính sách mới có quan hệ trực tiếp đến các mô hình blockchain chuyên biệt. Vì vậy, thành phố có điều kiện đề nghiên cứu, thử nghiệm và từng bước triển khai một số sản phẩm chuyên biệt gắn với tài chính số, TSMH theo cơ chế riêng của IFC Việt Nam tại Đà Nẵng và cơ chế thử nghiệm có kiểm soát (sandbox); Ủy ban nhân dân (UBND) thành phố thực hiện vai trò điều phối địa phương và tạo điều kiện hạ tầng trong phạm vi thẩm quyền.

Các mô hình chuyên biệt thực hiện theo cơ chế riêng của IFC Việt Nam tại Đà Nẵng theo khung pháp luật chuyên ngành và theo lộ trình giai đoạn 2028-2030 của Đề án; tổ chức được cấp phép cung cấp dịch vụ trong IFC không tự động được cung cấp dịch vụ cho khách hàng ngoài phạm vi IFC. Đối với các mô hình đã được cấp Giấy chứng nhận thử nghiệm có kiểm soát theo Nghị quyết số 55/2024/NQ-HĐND và đã đi vào vận hành từ trước, việc tiếp tục triển khai trong phạm vi, đối tượng và thời gian thử nghiệm được thực hiện theo quyết định đã cấp; trường hợp mở rộng ra ngoài phạm vi sandbox hoặc chuyển sang triển khai chính thức - doanh nghiệp cung cấp dịch vụ phải được cơ quan có thẩm quyền cấp phép hoặc theo quyết định của cơ quan có thẩm quyền.

4. Một số tồn tại, hạn chế trong triển khai hiện nay

Trong thời gian qua, thành phố và một số cơ quan, đơn vị đã có các nghiên cứu, đề xuất và thử nghiệm bước đầu đối với blockchain trong các lĩnh vực như ghi nhận dữ liệu, thanh toán số và một số mô hình dịch vụ mới. Tuy nhiên, các hoạt động này phần lớn vẫn

mang tính rời rạc, chưa hình thành một kiến trúc thống nhất, chưa có hạ tầng blockchain dùng chung, chưa có khung tích hợp, tiêu chuẩn chung, chưa có cơ chế tiếp nhận ứng dụng và cơ chế đánh giá hiệu quả ở quy mô toàn thành phố.

Mặt khác, mức độ số hoá và liên thông dữ liệu của thành phố ngày càng tăng, làm phát sinh rõ hơn nhu cầu xác minh, đối soát, truy vết, kiểm chứng trạng thái xử lý và làm rõ trách nhiệm trong môi trường số. Trong khi đó, hệ thống hiện hành chưa có một lớp nền tảng kỹ thuật chuyên biệt, thống nhất để hỗ trợ các yêu cầu này. Thành phố đồng thời còn đối mặt với các khoảng trống về chuẩn hóa dữ liệu nguồn diện rộng, cơ chế tích hợp, năng lực vận hành blockchain chuyên sâu, nguồn nhân lực, hệ sinh thái doanh nghiệp và cả năng lực điều phối liên ngành trong quá trình triển khai.

5. Điều kiện và tiền đề của thành phố

Đà Nẵng đã có những điều kiện quan trọng để xem xét triển khai blockchain theo hướng có chọn lọc, như cơ chế chính sách đặc thù theo Nghị quyết số 136/2024/QH15 và Nghị quyết số 259/2025/QH15 của Quốc hội; đã hình thành nền tảng hạ tầng số, dữ liệu, nền tảng tích hợp dùng chung và hệ sinh thái đổi mới sáng tạo tương đối phát triển; đồng thời nguồn nhân lực công nghệ thông tin và các cơ sở đào tạo đủ khả năng tham gia vào quá trình chuẩn bị, triển khai các ứng dụng ban đầu.

Về mặt định hướng chính sách, thành phố đã xác định blockchain là một trong ba trụ cột của kinh tế số cùng với robot và trí tuệ nhân tạo, theo Đề án Chuyển đổi số góp phần thúc đẩy, tạo động lực phát triển kinh tế - xã hội thành phố giai đoạn 2026-2030, định hướng đến năm 2035 tại Quyết định số 3292/QĐ-UBND ngày 30/12/2025 của UBND thành phố. Thành phố cũng đã có kinh nghiệm bước đầu trong tiếp nhận, tổ chức thử nghiệm và giám sát một số mô hình công nghệ mới trong khuôn khổ cơ chế sandbox theo Nghị quyết số 55/2024/NQ-HĐND. Đây là các tiền đề quan trọng để chuyển từ giai đoạn tiếp cận, nghiên cứu và thử nghiệm sang giai đoạn triển khai có hệ thống, có nền tảng dùng chung và có cơ chế quản trị rõ ràng.

6. Sự cần thiết ban hành Đề án

Từ các bối cảnh và tiền đề nêu trên, việc xây dựng và ban hành Đề án Thúc đẩy ứng dụng và phát triển công nghệ blockchain trên địa bàn thành phố Đà Nẵng là rất cần thiết để tổ chức thực hiện các nhiệm vụ được giao cho địa phương trong Chiến lược quốc gia về ứng dụng và phát triển công nghệ chuỗi khối (blockchain) đến năm 2025, định hướng đến năm 2030 và cụ thể hoá các nội dung thúc đẩy phát triển kinh tế số trong Đề án Chuyển đổi số thành phố. Đồng thời, Đề án tạo cơ sở để thành phố xác định những nhiệm vụ cần ưu tiên để hình thành hạ tầng blockchain dùng chung của thành phố, lựa chọn lĩnh vực ưu tiên cần ứng dụng công nghệ blockchain, chuẩn hóa điều kiện triển khai, phân định rõ phạm vi quản lý nhà nước, huy động sự tham gia của khu vực tư nhân và chuẩn bị chủ động về nguồn lực, nhân lực, dữ liệu và quản trị rủi ro.

CHƯƠNG II: HIỆN TRẠNG, XU HƯỚNG VÀ KINH NGHIỆM ỨNG DỤNG BLOCKCHAIN

I. HIỆN TRẠNG VÀ KINH NGHIỆM QUỐC TẾ

1. Kinh nghiệm ứng dụng blockchain trong dữ liệu tin cậy và dịch vụ công

Kinh nghiệm quốc tế cho thấy blockchain đóng vai trò lớp tin cậy số bổ sung để hỗ trợ xác minh, kiểm chứng, truy vết và đối soát giữa nhiều chủ thể. Trong mô hình này, dữ liệu nghiệp vụ vẫn được quản lý tại các hệ thống nguồn theo đúng chức năng và thẩm quyền; blockchain chỉ ghi nhận bằng chứng, dữ liệu tham chiếu và dữ liệu tối thiểu cần thiết.

a) Estonia

Estonia sử dụng công nghệ blockchain KSI (Keyless Signature Infrastructure) tích hợp với nền tảng trao đổi dữ liệu X-Road để tạo lập lớp tin cậy số cho Chính phủ điện tử. Nền tảng X-Road đảm nhận trao đổi dữ liệu giữa các cơ quan theo thẩm quyền và mục đích sử dụng, có ghi nhận nhật ký truy cập phục vụ hậu kiểm; trong khi blockchain KSI ghi nhận bằng chứng toàn vẹn, cho phép kiểm chứng độc lập các thay đổi dữ liệu và chỉ lưu giá trị băm chứ không lưu nội dung cá nhân. Nguyên tắc cốt lõi của mô hình là dữ liệu nguồn nằm tại từng cơ quan, KSI ghi giá trị băm trên chuỗi, hạn chế tối đa việc sao chép dữ liệu cá nhân giữa các hệ thống.

Với mô hình này, Estonia đã triển khai nhiều dịch vụ số trọng yếu: 100% đơn thuốc điện tử; khoảng 99% dân số có hồ sơ sức khỏe điện tử có thể truy cập toàn quốc; 98% doanh nghiệp thành lập trực tuyến trong khoảng 3 giờ; 100% tờ khai thuế trực tuyến trung bình trong khoảng 3 phút; các chương trình bỏ phiếu điện tử và e-Residency; nền tảng X-Road xử lý khoảng 2,7 tỷ truy vấn dữ liệu mỗi năm. Qua 20 năm triển khai, Estonia đã ghi nhận hơn 800 triệu chữ ký số, với lợi ích kinh tế ước tính khoảng 2% GDP; tính đến tháng 3/2025, Estonia có khoảng 1,4 triệu thẻ căn cước số hợp lệ và khoảng 232 nghìn người dùng Mobile-ID.

Kinh nghiệm rút ra cho Đà Nẵng:

- Phân vai rõ giữa nền tảng tích hợp dữ liệu và lớp tin cậy số; nền tảng xử lý trao đổi, blockchain ghi nhận bằng chứng, kiểm chứng và hậu kiểm.
- Dữ liệu nguồn luôn thuộc cơ quan quản lý chuyên ngành; blockchain chỉ lưu giá trị băm đủ để xác minh độc lập.
- Ưu tiên các bài toán có nhu cầu rõ về xác minh, truy vết và hậu kiểm; đây là nhóm bài toán blockchain phát huy giá trị rõ nhất trong khu vực công.
- Triển khai theo từng dịch vụ có dữ liệu đầy đủ và đầu mối rõ, gắn trực tiếp với nhóm bài toán dữ liệu tin cậy, xác minh, toàn vẹn và truy vết trong quản lý nhà nước.

b) Hàng Châu, Trung Quốc

Hàng Châu tổ chức hạ tầng blockchain hai lớp để phục vụ thành phố thông minh: lớp dùng chung kết nối với Mạng dịch vụ blockchain quốc gia của Trung Quốc, cung cấp

hạ tầng chuẩn hoá để triển khai nhanh các ứng dụng chính quyền điện tử; và lớp chuyên biệt qua Chuỗi khối Chiết Giang (Zhejiang Chain) kết nối trực tiếp với Tòa án Internet Hàng Châu. Cơ chế vận hành là các chứng cứ điện tử (hợp đồng số, ảnh chụp màn hình, tài liệu giao dịch) được tự động băm và gắn dấu thời gian trên Zhejiang Chain; các bên liên quan có thể kiểm chứng tính xác thực theo thời gian thực mà không cần liên hệ trực tiếp với cơ quan phát hành.

Mô hình này đã được mở rộng sang thanh toán bảo hiểm y tế, hoàn chi phúc lợi đô thị và các dịch vụ dân sự khác. Tòa án Internet Hàng Châu trở thành một trong những tòa án xử lý nhiều vụ kiện trực tuyến nhất; thời gian giải quyết tranh chấp thương mại điện tử được rút ngắn nhờ cơ chế xác minh bằng chứng tự động. Tính đến cuối năm 2023, Zhejiang Chain ghi nhận 568 giao dịch số với tổng giá trị khoảng 1,09 tỷ nhân dân tệ tại Trung tâm giao dịch số quốc tế Hàng Châu.

Kinh nghiệm rút ra cho Đà Nẵng:

- Mô hình hạ tầng blockchain dùng chung quốc gia (BSN) là tham chiếu trực tiếp cho Mạng dịch vụ blockchain đa chuỗi Việt Nam (VBSN). Đà Nẵng cần tổ chức DNC-Chain là thành phần triển khai cấp địa phương, kết nối, liên thông, đồng bộ với Nền tảng chuỗi khối quốc gia; và khả năng kết nối với các nền tảng chuỗi khối khác.

- Thí điểm hạ tầng blockchain trên một số bài toán có dữ liệu thật, có cơ quan chủ trì rõ ràng trước khi mở rộng phạm vi ứng dụng; bảo đảm đồng bộ, tránh chồng chéo, tiết kiệm và hiệu quả nguồn lực.

- Tổ chức blockchain theo hai lớp (một lớp dùng chung cho hạ tầng chuẩn hoá; một lớp chuyên biệt cho bài toán có yêu cầu nghiệp vụ và pháp lý đặc thù) là cách tiếp cận đáng tham khảo cho DNC-Chain.

- Tích hợp blockchain với tư pháp và hành chính có giá trị cho các bài toán toàn vẹn hồ sơ, bằng chứng điện tử, đối soát nhiều chủ thể và trách nhiệm giải trình.

- Giá trị của blockchain trong khu vực công nằm ở kiểm chứng và truy vết, không nằm ở thay thế toàn bộ hệ thống nghiệp vụ.

c) Thâm Quyển, Trung Quốc

Thâm Quyển tổ chức mạng blockchain có cấp phép kết nối cơ quan thuế (Cục Thuế tỉnh Quảng Đông) với doanh nghiệp theo kiến trúc phân tán nhiều nút. Mỗi hoá đơn điện tử khi phát hành được mã hoá, băm trên blockchain cùng với siêu dữ liệu người phát hành, người nhận, giá trị và mã tham chiếu. Bất kỳ bên liên quan nào (cơ quan thuế, đơn vị kiểm toán, đối tác kinh doanh) đều có thể kiểm chứng giá trị băm mà không cần liên hệ trực tiếp với cơ quan thuế.

Tính đến tháng 3/2021, theo công bố của Cục Thuế Thâm Quyển, hơn 47 triệu hoá đơn điện tử đã được xác minh trên blockchain với tổng giá trị hơn 600 tỷ nhân dân tệ; xác minh hoá đơn cho doanh nghiệp trong hơn 100 ngành nghề; cung cấp giao diện lập trình ứng dụng (API) cho doanh nghiệp tích hợp trực tiếp vào phần mềm kế toán nội bộ. Hành vi gian lận hoá đơn giảm rõ rệt; thời gian đối soát từ vài ngày rút xuống thời gian thực.

Kinh nghiệm rút ra cho Đà Nẵng:

- Blockchain phát huy hiệu quả đối với bài toán có khối lượng giao dịch lớn, nhu cầu xác minh và đối soát liên hệ thống cao, có quy trình rõ.

- Mô hình blockchain có cấp phép phù hợp với quản trị khu vực công khi chỉ chủ thể được cấp quyền mới tham gia kiểm chứng và khai thác.

- Hạ tầng thiết kế theo kiến trúc mở, có giao diện cho doanh nghiệp tích hợp là điều kiện quan trọng để mở rộng quy mô.

- Ưu tiên triển khai các ứng dụng có nhu cầu kiểm chứng cao, tần suất phát sinh lớn, quy trình rõ, dễ lượng hoá hiệu quả và có khả năng mở rộng sau thí điểm.

d) Busan, Hàn Quốc

Busan triển khai blockchain có cấp phép để xây dựng định danh số phi tập trung (DID) phục vụ dịch vụ hành chính không tiếp xúc. Mỗi công dân có một định danh số duy nhất; các chứng nhận được cấp dưới dạng chứng nhận có thể xác minh (Verifiable Credential) theo chuẩn W3C, lưu trong ứng dụng ví di động B-PASS. Kiến trúc này không tập trung dữ liệu cá nhân: người dùng kiểm soát thông tin của mình và chỉ chia sẻ phần thông tin cần thiết khi xuất trình chứng nhận, khoá bí mật cũng do người dùng giữ. Đến năm 2021, B-PASS có khoảng 100.000 lượt cài đặt và tích hợp khoảng 100 loại chứng nhận, giảm khối lượng xử lý giấy tờ tại các đơn vị hành chính.

Kinh nghiệm rút ra cho Đà Nẵng:

- Blockchain có thể hỗ trợ các bài toán định danh không tiếp xúc theo cách cân bằng giữa yêu cầu xác minh và yêu cầu hạn chế lộ dữ liệu cá nhân; blockchain đóng vai trò hỗ trợ xác minh, không phải kho lưu trữ dữ liệu cá nhân.

- Triển khai thử nghiệm trước khi nhân rộng đối với các ứng dụng mới liên quan đến định danh số, giấy tờ số và dữ liệu cá nhân; đánh giá kết quả trước khi mở rộng.

- Định danh số chỉ hiệu quả khi gắn với hệ sinh thái dịch vụ cụ thể; các công cụ như ví giấy tờ số và chứng thư số phải đi kèm với dịch vụ công, dịch vụ đô thị và quy trình nghiệp vụ thực tế.

2. Kinh nghiệm về tài chính số, TSMH và hệ sinh thái

Kinh nghiệm quốc tế cho thấy phát triển blockchain không chỉ là việc xây dựng một nền tảng kỹ thuật mà còn là quá trình hình thành hệ sinh thái gồm cơ quan quản lý, doanh nghiệp, tổ chức tài chính, cơ sở đào tạo, nghiên cứu, cộng đồng chuyên gia và người dùng. Trong hệ sinh thái này, các mô hình gắn với tài chính số và TSMH hiện là một trong những ứng dụng có quy mô kinh tế lớn nhất của blockchain. Nguyên tắc chung của các IFC hàng đầu là không mở rộng vô điều kiện đối với mô hình gắn với tài chính số và TSMH; mọi hoạt động tuân thủ khung pháp lý phù hợp, phân loại theo bản chất hoạt động, mức độ rủi ro và năng lực giám sát của cơ quan quản lý; tuân thủ khuyến nghị của Lực lượng đặc nhiệm tài chính (FATF) về phòng, chống rửa tiền, chống tài trợ khủng bố, chống tài trợ phổ biến vũ khí hủy diệt hàng loạt (AML/CFT/CTTPBVKHDHL). Các quốc gia có IFC đều xây dựng khung pháp lý tách biệt hoạt động trong IFC khỏi phần còn lại của khu vực tài phán: tổ chức được cấp phép cung cấp dịch vụ trong IFC không tự động được cung cấp dịch vụ cho khách hàng ngoài phạm vi IFC; mở rộng ra ngoài IFC

phải tuân thủ pháp luật chuyên ngành quốc gia hoặc quyết định của cơ quan có thẩm quyền.

a) Dubai, Các Tiểu vương quốc Ả-rập Thống nhất

Dubai áp dụng mô hình hai cơ quan quản lý tách biệt cho TSMH theo địa giới pháp lý. Trong Trung tâm tài chính quốc tế Dubai (DIFC), Cơ quan Dịch vụ tài chính Dubai (DFSA) cấp phép và giám sát mọi hoạt động tài chính bao gồm token tiền điện tử theo Crypto Token Regime; ngoài phạm vi DIFC, Cơ quan quản lý tài sản ảo Dubai (VARA) là cơ quan quản lý chuyên trách cho toàn bộ Emirate Dubai, áp dụng bộ quy tắc riêng và cấm phát hành token tăng tính ẩn danh. Hai cơ quan ký Bản ghi nhớ về Khuôn khổ hợp tác để bảo đảm phối hợp giám sát, không chồng chéo phạm vi và đồng bộ với chuẩn quốc tế. Theo công bố của DFSA, sửa đổi đối với Crypto Token Regime trong DIFC có hiệu lực từ ngày 12/01/2026, chuyển trách nhiệm chính trong đánh giá tính phù hợp của token tiền điện tử sang tổ chức được cấp phép, đồng thời tăng cường yêu cầu về quản trị, lưu ký, công bố thông tin và tuân thủ.

Kinh nghiệm rút ra cho Đà Nẵng:

- Phân định rõ phạm vi pháp lý trong và ngoài IFC là yêu cầu nền tảng để tổ chức thị trường TSMH; trong IFC Việt Nam tại Đà Nẵng, mô hình TSMH nên vận hành theo cơ chế riêng của IFC; ngoài phạm vi IFC, hoạt động TSMH tuân thủ Nghị quyết số 05/2025/NQ-CP của Chính phủ và pháp luật chuyên ngành quốc gia hoặc theo quyết định của cơ quan có thẩm quyền.

- Tổ chức được cấp phép cung cấp dịch vụ trong IFC không tự động được cung cấp dịch vụ cho khách hàng ngoài phạm vi IFC; mở rộng phạm vi phải có quyết định của cơ quan có thẩm quyền.

- Cơ chế phối hợp giữa các cơ quan quản lý phải được thiết lập từ đầu để giảm chồng chéo và bảo đảm tuân thủ AML/CFT/CTTPBVKHDHL.

b) Hồng Kông, Trung Quốc

Tháng 6/2025, Hồng Kông ban hành Tuyên bố chính sách về Tài sản kỹ thuật số phiên bản 2.0 với định hướng xây dựng hệ sinh thái tài sản số minh bạch, tin cậy, tăng cường bảo vệ nhà đầu tư và quản trị rủi ro thị trường. Pháp lệnh về Stablecoin có hiệu lực từ ngày 01/8/2025 yêu cầu phát hành stablecoin phải có giấy phép; các nền tảng giao dịch TSMH tiếp tục được cấp phép và công khai trạng thái minh bạch. Đến thời điểm ban hành pháp lệnh, đã cấp 9 giấy phép và có 8 hồ sơ đang xem xét.

Song song, thị trường token hoá tài sản thực được thúc đẩy qua Chương trình Hỗ trợ Trái phiếu Kỹ thuật số và trợ cấp tối đa 2,5 triệu HKD cho mỗi đợt phát hành. Tháng 11/2025, Hồng Kông thực hiện đợt phát hành trái phiếu xanh số hoá thứ ba. Trong nửa đầu năm 2025, giá trị giao dịch liên quan đến TSMH và token hoá tại các định chế tài chính đạt khoảng 26,1 tỷ HKD, tăng 233% so với cùng kỳ. Bên cạnh tăng trưởng thị trường, Hồng Kông tăng cường yêu cầu AML/CFT/CTTPBVKHDHL và thiết lập cơ chế chia sẻ thông tin giữa cơ quan quản lý và các tổ chức tài chính; theo công bố của Cảnh sát Hồng Kông, năm 2024 ghi nhận 44.480 vụ lừa đảo (tăng 11,7% so với 2023), trong đó hình thức lừa đảo đầu tư gắn với TSMH là một trong những phương thức phổ biến; các

yêu cầu về tách bạch tài sản khách hàng, kiểm toán độc lập, truy vết giao dịch và thực thi FATF Travel Rule đang được siết chặt.

Kinh nghiệm rút ra cho Đà Nẵng:

- Khung pháp lý song hành phát triển thị trường, công khai tình trạng pháp lý và phân loại hoạt động là yêu cầu nền tảng để kiểm soát rủi ro và bảo vệ người dùng.
- Yêu cầu tuân thủ AML/CFT/CTTPBVKHDHL là bắt buộc đối với mọi mô hình chuyên biệt; mô hình tích hợp sẵn cơ chế KYC, lưu vết giao dịch, giám sát giao dịch bất thường và cung cấp thông tin phục vụ kiểm tra, xác minh.tr
- Token hoá trong thị trường vốn chỉ là định hướng đối với nhóm mô hình chuyên biệt gắn IFC, không áp dụng đại trà cho hạ tầng dùng chung của thành phố.

c) Singapore

Singapore áp dụng nguyên tắc quản lý theo bản chất hoạt động, không theo tên công nghệ. Luật Dịch vụ thanh toán yêu cầu các dịch vụ token thanh toán số phải có giấy phép, tập trung vào bản chất dịch vụ tài chính và mức độ rủi ro. Đến đầu năm 2026, theo công bố của Cơ quan Quản lý Tiền tệ Singapore (MAS), đã có 36 giấy phép tổ chức thanh toán lớn (Major Payment Institution) cho dịch vụ token thanh toán số; danh sách giấy phép công khai cho phép kiểm chứng trạng thái pháp lý và giám sát trên cơ sở dữ liệu. Singapore cũng hoàn thiện yêu cầu đối với stablecoin như dự trữ đầy đủ, tách bạch tài sản khách hàng, kiểm toán độc lập, có khả năng mua lại theo mệnh giá trong vòng tối đa 5 ngày làm việc.

Đối với token hoá RWA, Singapore triển khai thí điểm qua cơ chế hợp tác công - tư, tập trung vào công cụ nợ và nâng cấp hạ tầng thị trường vốn; tháng 11/2025, lần đầu tiên Singapore phê duyệt phân phối quỹ mở cho nhà đầu tư cá nhân theo hình thức token hoá. Đến ngày 30/6/2025, đã áp dụng quy định quản lý dành riêng cho các nhà cung cấp dịch vụ TSMH chỉ phục vụ ngoài nước, duy trì quan điểm thận trọng đối với rủi ro xuyên biên giới.

Kinh nghiệm rút ra cho Đà Nẵng:

- Quản lý theo bản chất hoạt động, không theo tên gọi công nghệ; phân loại các mô hình và dịch vụ liên quan theo mức độ rủi ro và yêu cầu quản lý.
- Công khai tình trạng pháp lý của chủ thể tham gia để tăng minh bạch, hỗ trợ giám sát và hạn chế rủi ro đối với người sử dụng và cơ quan quản lý.
- Yêu cầu về dự trữ bảo chứng, tách bạch tài sản, kiểm toán độc lập và nghĩa vụ hoàn trả đối với các mô hình có yếu tố stablecoin hoặc giá trị số ổn định.

d) Lugano, Thụy Sĩ

Thụy Sĩ là một trong những quốc gia sớm nhất có khung pháp lý cho giao dịch TSMH và công nghệ sổ cái phân tán từ năm 2021, tạo cơ sở pháp lý cho việc phát hành, giao dịch và xử lý các công cụ tài chính trên sổ cái phân tán. Trên cơ sở đó, Lugano triển khai chương trình Plan B với trọng tâm mở rộng chấp nhận thanh toán TSMH cho các

nghĩa vụ nộp phí và nghĩa vụ với chính quyền đô thị, kết hợp phát triển mạng lưới các điểm chấp nhận thanh toán.

Theo công bố của chính quyền Lugano, đã có hơn 360 điểm chấp nhận Bitcoin và USDT; Diễn đàn Plan B năm 2024 thu hút hơn 2.900 người tham dự; trong một tuần, các điểm chấp nhận ghi nhận khoảng 8.000 giao dịch trên chuỗi. Cơ chế quản trị rủi ro tài chính đáng chú ý: chính quyền không trực tiếp nắm giữ TSMH; dòng thanh toán được tổ chức qua cơ chế chuyển đổi tự động thông qua trung gian, quy đổi sang franc Thụy Sĩ và ghi nhận vào luồng ngân sách, qua đó hạn chế rủi ro tỷ giá, lưu ký và biến động giá. Ngoài ra, Lugano đã phát hành trái phiếu đô thị số hoá: 100 triệu CHF năm 2023 kỳ hạn 6 năm lãi suất 1,625%; 100 triệu CHF năm 2024 kỳ hạn 10 năm lãi suất 1,415% trong khung thử nghiệm của Ngân hàng Quốc gia Thụy Sĩ.

Kinh nghiệm rút ra cho Đà Nẵng:

- Các mô hình TSMH ở cấp thành phố chỉ phù hợp khi có khung pháp lý rõ và hạ tầng thị trường được quản lý; chính quyền không trực tiếp nắm giữ TSMH mà sử dụng cơ chế chuyển đổi tự động qua trung gian, hạn chế rủi ro tỷ giá, lưu ký và biến động giá.

- TSMH trong môi trường đô thị chỉ có ý nghĩa khi gắn với kịch bản sử dụng thực tế: phí, nghĩa vụ, dịch vụ đô thị, thanh toán tại cơ sở kinh doanh và các giao dịch có thể kiểm chứng.

- Token hoá trái phiếu đô thị là hướng tham chiếu có giá trị đối với phát triển dài hạn khi có đủ điều kiện về pháp lý, hạ tầng giao dịch được quản lý, cơ chế giám sát, kiểm toán, xếp hạng tín nhiệm và quản trị nợ công phù hợp.

- Các thử nghiệm triển khai trong phạm vi hẹp, có kiểm soát, phù hợp với nhóm sản phẩm chuyên biệt gắn IFC hoặc sandbox; không áp dụng cho nhóm ứng dụng dùng chung của thành phố.

3. Rủi ro và bài học kinh nghiệm từ thực tiễn quốc tế

Tổ chức Hợp tác và Phát triển Kinh tế (OECD) nhận định blockchain không phải là công nghệ áp dụng đồng bộ ở mọi quốc gia, địa phương và ngành nghề; hiệu quả triển khai phụ thuộc vào chất lượng dữ liệu, độ trưởng thành của hạ tầng số, khung pháp lý, cơ chế quản trị, năng lực tích hợp và năng lực tổ chức thực hiện. Số lượng dự án thoát khỏi giai đoạn thí điểm để tạo tác động rõ nét vẫn còn hạn chế.

Đối với các mô hình blockchain phục vụ dữ liệu tin cậy và dịch vụ công, blockchain không thay thế được chất lượng dữ liệu nguồn. Kinh nghiệm Estonia, Hàng Châu, Thẩm Quyển và Busan đều cho thấy dữ liệu nghiệp vụ phải được quản lý tại các hệ thống nguồn; blockchain chỉ phát huy giá trị khi đóng vai trò lớp bổ sung ghi nhận bằng chứng, hỗ trợ kiểm chứng và truy vết. Nếu dữ liệu nguồn chưa chuẩn hóa, chưa đầy đủ, chưa có đầu mối quản lý rõ hoặc chưa có khả năng tích hợp, việc đưa blockchain vào sẽ làm tăng độ phức tạp mà không tạo được hiệu quả tương xứng.

Xây dựng nền tảng blockchain chỉ là một phần; phần khó hơn là tích hợp nền tảng vào quy trình nghiệp vụ và hạ tầng lõi. Trường hợp tiêu biểu là dự án thay thế hệ thống CHESS của Sở Giao dịch Chứng khoán Úc: phần mềm mới đạt khoảng 63% tiến độ hoàn

thành, phát sinh nhiều vấn đề về khả năng hỗ trợ, khả năng mở rộng, độ ổn định và năng lực quản lý dự án, dẫn đến ghi giảm giá trị phần mềm vốn hoá khoảng 245-255 triệu đô la Úc trước thuế. Đây là cảnh báo rõ khi ngay cả ở môi trường thể chế phát triển, việc tích hợp blockchain vào hạ tầng lõi vẫn mang theo rủi ro thiết kế, rủi ro tiến độ, rủi ro chi phí và rủi ro vận hành đáng kể.

Việc mở rộng quy mô phụ thuộc vào hạ tầng dùng chung, tiêu chuẩn tích hợp và sự phân vai rõ ràng giữa hệ thống nguồn, nền tảng tích hợp và blockchain. Nếu mỗi cơ quan triển khai riêng, thiếu tiêu chuẩn kết nối, thiếu cơ chế kiểm tra tuân thủ và thiếu cơ chế quản lý vòng đời ứng dụng, blockchain sẽ dừng ở các thử nghiệm rời rạc, khó mở rộng và khó đo lường hiệu quả.

Đối với hoạt động ứng dụng blockchain nói chung, blockchain làm tăng đáng kể yêu cầu về chuẩn hóa dữ liệu, kiểm soát truy cập, ghi nhật ký, giám sát vận hành, kiểm tra tuân thủ và xử lý sự cố. Nếu các tiền đề này chưa đủ, blockchain sẽ trở thành một lớp công nghệ phủ lên mà không tạo giá trị tương xứng. Blockchain chỉ phát huy hiệu quả khi áp dụng cho các bài toán có nhu cầu xác minh, truy vết, đối soát hoặc chia sẻ dữ liệu tin cậy giữa nhiều chủ thể; không nên áp dụng cho lĩnh vực mà dữ liệu chưa đủ độ tin cậy, quy trình chưa rõ hoặc chưa có nhu cầu xác minh giữa nhiều bên.

Đối với các mô hình gắn với tài chính số và TSMH, mức độ rủi ro cao hơn đáng kể so với nhóm dữ liệu tin cậy và dịch vụ công. Ủy ban Ổn định Tài chính (FSB) nhận định khung pháp lý cho TSMH và stablecoin tại các quốc gia chưa hoàn chỉnh, chưa đồng đều, dẫn đến khoảng trống giám sát và nguy cơ chênh lệch quy định. Sự đổ vỡ của sàn giao dịch tài sản số như FTX hay vụ tấn công bảo mật vào sàn Bybit đầu năm 2025 (thiệt hại khoảng 1,5 tỷ USD) là bài học thực tiễn cho các thị trường đang phát triển.

Tội phạm và rủi ro an ninh cũng gia tăng cùng quy mô. Theo Báo cáo Tội phạm Tiền điện tử của Chainalysis năm 2025, tổng giá trị giao dịch bất hợp pháp trên blockchain năm 2024 ban đầu được ghi nhận khoảng 40,9 tỷ USD và có thể đạt khoảng 51 tỷ USD sau khi tiếp tục phát hiện các giao dịch liên quan; đến giữa năm 2025, giá trị bị đánh cắp từ các dịch vụ TSMH vượt 2,17 tỷ USD; stablecoin chiếm khoảng 84% khối lượng giao dịch bất hợp pháp; các mạng lưới rửa tiền xuyên quốc gia sử dụng khoảng 16,1 tỷ USD quỹ bất hợp pháp thông qua giao dịch TSMH trong năm 2025. Theo cập nhật của FATF tháng 6/2025 (lần thứ sáu) về thực hiện Khuyến nghị 15 đối với TSMH và nhà cung cấp dịch vụ TSMH, 67 quốc gia chiếm khoảng 98% hoạt động dịch vụ TSMH toàn cầu đã được rà soát; gần một phần ba chưa thông qua luật thực hiện FATF Travel Rule. Vì vậy, thị trường TSMH đòi hỏi năng lực giám sát, truy vết dòng tiền, ATTT, ANM và bảo vệ nhà đầu tư vượt xa mặt bằng chung; các điều kiện này phải được bảo đảm trước khi triển khai trên diện rộng.

II. HIỆN TRẠNG VÀ XU HƯỚNG TẠI VIỆT NAM

1. Bối cảnh pháp lý, dữ liệu và yêu cầu liên thông

Khung pháp lý về dữ liệu, giao dịch điện tử, BVDLCN và quản trị dữ liệu đang từng bước hoàn thiện theo hướng chuẩn hóa, liên thông và tăng cường trách nhiệm quản lý dữ liệu trong toàn hệ thống chính trị. Nghị định số 278/2025/NĐ-CP về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan là dấu mốc quan trọng. Hệ thống pháp luật về dữ liệu và

CĐS tiếp tục được định hình bởi Luật Giao dịch điện tử số 20/2023/QH15, Luật Dữ liệu số 60/2024/QH15, Luật BVĐLCN số 91/2025/QH15, Luật Công nghiệp công nghệ số số 71/2025/QH15 và Luật Chuyển đổi số số 148/2025/QH15. Đây là xu hướng có ý nghĩa trực tiếp đối với ứng dụng blockchain, vì blockchain chỉ phát huy hiệu quả khi được đặt trong một môi trường có dữ liệu chuẩn, có cơ chế chia sẻ, phân định trách nhiệm và cơ sở pháp lý đủ rõ.

Bên cạnh đó, yêu cầu liên thông dữ liệu và kiểm chứng trạng thái xử lý ngày càng trở nên rõ nét. Khi dữ liệu được tạo lập và chia sẻ trên quy mô lớn, nhu cầu không chỉ dừng ở kết nối kỹ thuật mà mở rộng sang xác minh nguồn gốc, kiểm chứng tính toàn vẹn, truy vết quá trình xử lý và làm rõ trách nhiệm giữa các chủ thể tham gia. Đây là tiền đề quan trọng để các công nghệ như blockchain đóng vai trò công cụ hỗ trợ cho các bài toán phù hợp. Dù vậy, việc hình thành không gian chính sách không đồng nghĩa mọi mô hình blockchain đều đã có đủ hành lang triển khai. Trong điều kiện hiện nay, việc lựa chọn ứng dụng blockchain vẫn phải gắn với điều kiện dữ liệu nguồn, điều kiện pháp lý chuyên ngành, mức độ sẵn sàng của hạ tầng và khả năng quản trị rủi ro của từng cơ quan, từng địa phương.

2. Xu hướng phát triển hạ tầng blockchain và mô hình dùng chung

Giai đoạn 2020-2025 cho thấy năng lực blockchain trong nước đã từng bước hình thành ở cả lớp ứng dụng và lớp nền tảng. Các ứng dụng đã được phát triển và thử nghiệm như: hệ thống xác minh văn bằng, chứng chỉ của Học viện Công nghệ Bưu chính Viễn thông; và nhiều giải pháp xác minh, kiểm chứng dữ liệu do doanh nghiệp và tổ chức trong nước phát triển. Xu hướng quan sát được là sự chuyển dịch từ triển khai đơn lẻ theo từng tổ chức sang mô hình hạ tầng dùng chung với mức độ chuẩn hoá và liên thông cao.

Một ví dụ đáng chú ý là ứng dụng VNIDCheck cho truy xuất nguồn gốc tiền chất, hóa chất bằng VNeID trên mạng blockchain VNIDChain, được tích hợp trong Mạng dịch vụ blockchain đa chuỗi Việt Nam (VBSN), mô hình kiến trúc đang được xem xét lựa chọn làm Nền tảng chuỗi khối quốc gia. Theo mô hình tham chiếu này, khung kiến trúc đa chuỗi blockchain permissioned Layer-1 phục vụ kết nối, tiêu chuẩn hoá và hỗ trợ liên thông giữa các blockchain thành phần, giúp các tổ chức tự xây dựng, vận hành blockchain thành phần nhưng vẫn liên thông trong không gian chung với tiêu chuẩn đáp ứng điều kiện kỹ thuật, an toàn, an ninh và pháp lý phù hợp. Xu hướng này cho thấy blockchain trong nước đang được nhìn nhận như một nền tảng phục vụ các nhu cầu xác minh, truy xuất, kiểm chứng và hỗ trợ liên thông dữ liệu, không đơn thuần là công nghệ dành cho TSMH hay giao dịch tài chính số.

3. Xu hướng tài chính số, TSMH và sandbox tại Việt Nam

Theo báo cáo của Triple-A năm 2024, Việt Nam là một trong những quốc gia có số lượng người nắm giữ TSMH lớn, ước tính khoảng 17 triệu người; theo báo cáo của Chainalysis, giá trị giao dịch giai đoạn tháng 7/2024 đến tháng 6/2025 đạt khoảng 220 tỷ USD. Các dự án do người sáng lập và nguồn gốc Việt Nam đạt quy mô đáng kể, một số dự án được định giá hàng tỷ USD. Tuy nhiên, phần lớn các dự án này vận hành trên logic thị trường toàn cầu (phát hành token, trò chơi blockchain) và không có tác động trực tiếp đến hệ sinh thái và hạ tầng trong nước.

Song song, rủi ro gian lận và lừa đảo gia tăng. Năm 2024, thiệt hại do lừa đảo trực tuyến tại Việt Nam ước tính khoảng 18.900 tỷ đồng, trong đó mời gọi đầu tư qua TSMH là một trong những phương thức phổ biến. Thực tế gần đây, cơ quan chức năng đã triệt phá nhiều vụ việc lớn liên quan đến mô hình đầu tư lợi dụng công nghệ blockchain và TSMH để huy động vốn và chiếm đoạt tài sản, như đường dây lừa đảo đầu tư TSMH 51 triệu USDT (tương đương khoảng 1.275 tỷ đồng) bị phát hiện tại Đắk Lắk cuối năm 2025, hay vụ án quy mô rất lớn liên quan đến "Mr Pips".

Trong bối cảnh đó, năm 2025 ghi nhận những tiến triển quan trọng khi Chính phủ ban hành Nghị quyết số 05/2025/NQ-CP về thí điểm thị trường TSMH trong 5 năm; Nghị quyết số 222/2025/QH15 của Quốc hội và Nghị định số 323/2025/NĐ-CP của Chính phủ là nền tảng hình thành IFC Việt Nam đặt tại Thành phố Hồ Chí Minh và thành phố Đà Nẵng; Nghị định số 329/2025/NĐ-CP của Chính phủ quy định cụ thể về AML/CFT/CTTPBVKHDHL trong IFC. Theo khoản 2 Điều 51 Luật Đầu tư số 143/2025/QH15, kể từ ngày 01/7/2026, hoạt động cung cấp dịch vụ liên quan TSMH thuộc danh mục ngành, nghề đầu tư kinh doanh có điều kiện. Các văn bản này cho thấy hệ sinh thái blockchain và tài chính số tại Việt Nam đang được tiếp cận như một không gian phát triển mới, gắn với cơ chế quản lý chuyên ngành trong khuôn khổ phát triển IFC và cơ chế sandbox.

III. HIỆN TRẠNG VÀ MỨC ĐỘ SẴN SÀNG CỦA ĐÀ NẴNG

1. Điều kiện thể chế và cơ chế triển khai

Thành phố Đà Nẵng có các điều kiện thể chế tương đối thuận lợi để nghiên cứu, thử nghiệm và từng bước triển khai các mô hình công nghệ mới khi được Quốc hội thông qua các cơ chế, chính sách đặc thù tại Nghị quyết số 136/2024/QH15 và Nghị quyết số 259/2025/QH15. Trên cơ sở đó, thành phố đã ban hành các văn bản điều hành quan trọng như Kế hoạch hành động số 21-KH/TU ngày 10/9/2025 của Ban Thường vụ Thành ủy thực hiện Nghị quyết số 57-NQ/TW, Kế hoạch số 122/KH-UBND của UBND thành phố, Quyết định số 3292/QĐ-UBND phê duyệt Đề án CDS giai đoạn 2026-2030 và Quyết định số 3291/QĐ-UBND ban hành Khung kiến trúc số.

Thành phố cũng đã thiết lập cơ chế sandbox đối với các giải pháp công nghệ mới theo Nghị quyết số 55/2024/NQ-HĐND của Hội đồng nhân dân (HĐND) thành phố, tạo cơ sở pháp lý cho việc tiếp nhận, thẩm định và tổ chức triển khai thử nghiệm. Thực tế, một số mô hình có yếu tố blockchain và TSMH đã được cấp Giấy chứng nhận sandbox trong khuôn khổ này, bước đầu hình thành năng lực tổ chức thử nghiệm, quản lý, giám sát và đánh giá các mô hình công nghệ mới.

Bên cạnh đó, Đà Nẵng đã ban hành một số chính sách hỗ trợ liên quan đến ĐMST, phát triển hạ tầng công nghệ và nguồn nhân lực, như miễn, giảm thuế cho hoạt động ĐMST theo Nghị quyết số 53/2024/NQ-HĐND, hỗ trợ không hoàn lại cho nghiên cứu, phát triển theo Nghị quyết số 54/2024/NQ-HĐND, phát triển nguồn nhân lực vi mạch bán dẫn và trí tuệ nhân tạo theo Nghị quyết số 57/2024/NQ-HĐND và hỗ trợ hạ tầng công nghệ thông tin theo Nghị quyết số 58/2024/NQ-HĐND. Dù không được thiết kế riêng cho blockchain, các chính sách này góp phần tạo điều kiện về nguồn lực, nhân lực, hạ tầng và môi trường triển khai cho các giải pháp công nghệ mới trên địa bàn.

Thành phố đã bước đầu tiếp nhận, thẩm định, cho phép thử nghiệm và giám sát một số mô hình có yếu tố blockchain theo cơ chế sandbox. Thực tế này cho thấy Đà Nẵng đã có cơ sở để bước sang giai đoạn tổ chức triển khai theo định hướng thống nhất hơn. Tuy nhiên, khuôn khổ pháp lý hiện hành chủ yếu phục vụ thử nghiệm theo từng trường hợp, chưa đủ để hình thành một cơ chế thống nhất cho việc tiếp nhận ứng dụng ở quy mô thành phố, cho quản trị dữ liệu trên blockchain và cho quản lý vòng đời ứng dụng. Vì vậy, về mặt thể chế, thành phố có nền tảng ban đầu, nhưng vẫn cần xây dựng bổ sung và chuẩn hoá các điều kiện để triển khai một cách đồng bộ.

2. Hạ tầng số, dữ liệu và nền tảng tích hợp dùng chung

Thành phố Đà Nẵng đã hình thành nền tảng hạ tầng số và dữ liệu tương đối đồng bộ. Sau sáp nhập đơn vị hành chính cấp tỉnh, thành phố Đà Nẵng (mới) được hình thành trên cơ sở sáp nhập thành phố Đà Nẵng (cũ) và tỉnh Quảng Nam, kế thừa 02 trung tâm dữ liệu (TTDL) nhà nước trên địa bàn: TTDL chính tại Công viên phần mềm số 1 (phường Hải Châu) với 165 máy chủ vật lý, TTDL dự phòng tại Tam Kỳ với 54 máy chủ vật lý. Cụm 02 TTDL nhà nước phân tán tại Hải Châu và Tam Kỳ tạo điều kiện thuận lợi để tổ chức hạ tầng kỹ thuật theo nguyên tắc phân tán về địa lý, dự phòng chéo và bảo đảm liên tục vận hành. Do TTDL chính tại Công viên phần mềm số 1 đã gần hết dư địa mở rộng vật lý và TTDL dự phòng tại Tam Kỳ còn nhiều dư địa, việc bố trí hạ tầng mới cần ưu tiên khai thác dư địa của TTDL dự phòng tại Tam Kỳ, kết hợp tái cấu hình hợp lý TTDL chính theo chu kỳ nâng cấp, thay thế thiết bị.

Trên địa bàn cũng đã có sự tham gia của các TTDL doanh nghiệp như VNPT, Viettel, CMC, FPT và các dự án TTDL mới đang được triển khai; riêng giai đoạn 2025-2027 sẽ có thêm hai TTDL quốc tế mới với tổng quy mô khoảng 2.000 rack đã và đang đưa vào vận hành. Thành phố cũng có hạ tầng truyền dẫn và viễn thông tương đối ổn định, với mạng đô thị khoảng 450 km cáp quang ngầm kết nối 192 cơ quan nhà nước, mạng truyền số liệu chuyên dùng đã kết nối 100% cơ quan hành chính, tỷ lệ phủ sóng 4G đạt 99%, 5G đạt 75% và tốc độ truy nhập băng rộng di động trung bình đạt 90,32 Mb/s.

Về nền tảng số, dữ liệu và mức độ liên thông, Đà Nẵng đã bước sang giai đoạn vận hành các dịch vụ công và chia sẻ dữ liệu số ở quy mô lớn. Thành phố hiện cung cấp 2.118 dịch vụ công trực tuyến trên tổng số 2.226 thủ tục hành chính, đạt khoảng 95%; tỷ lệ hồ sơ trực tuyến đạt 77,5%; nền tảng tích hợp và chia sẻ dữ liệu xử lý bình quân khoảng 1.000.000 giao dịch mỗi ngày; đã phát triển 1.474 dịch vụ chia sẻ dữ liệu qua giao diện lập trình ứng dụng và ghi nhận lũy kế hơn 1,2 triệu lượt gọi API. Khối lượng dữ liệu đang được quản lý cũng ở quy mô lớn, gồm 2.580.552 trường hợp hộ tịch điện tử, 30.606 hồ sơ cán bộ, công chức, viên chức và hơn 1.100.000 dữ liệu đặc tả kho lưu trữ số.

Thành phố Đà Nẵng cơ bản đáp ứng hạ tầng để triển khai các bài toán về toàn vẹn hồ sơ, xác minh, truy xuất, đối soát liên hệ thống và khai thác dữ liệu tin cậy. Việc kế thừa 02 TTDL nhà nước phân bố tại Hải Châu và Tam Kỳ bảo đảm khả năng phân tán về địa lý giữa các địa điểm độc lập, là điều kiện kỹ thuật thuận lợi cho triển khai hạ tầng blockchain dùng chung có tính chất phân tán, chịu lỗi và bảo đảm liên tục vận hành. Tuy vậy, mức độ chuẩn hoá dữ liệu giữa các hệ thống nguồn chưa đồng đều; quá trình hợp

nhất, chuẩn hoá dữ liệu sau sáp nhập đơn vị hành chính đang được thực hiện theo lộ trình; năng lực mở rộng của một số hạ tầng nhà nước còn hạn chế. Do đó, hạ tầng số và dữ liệu của thành phố cơ bản đủ cho giai đoạn triển khai ban đầu có chọn lọc, chưa sẵn sàng để mở rộng ngay ở quy mô lớn. Đối với dữ liệu, cần tổ chức chuẩn hóa trước khi đưa vào tích hợp.

3. Hệ sinh thái doanh nghiệp, cơ sở đào tạo, tổ chức hỗ trợ

Đà Nẵng có môi trường ĐMST và công nghệ số tương đối phát triển, với hệ sinh thái doanh nghiệp công nghệ số, các tổ chức hỗ trợ khởi nghiệp ĐMST, các sự kiện công nghệ lớn và mạng lưới hợp tác trong nước, quốc tế bước đầu được hình thành.

Hệ sinh thái của thành phố đang phát triển với mật độ doanh nghiệp công nghệ số khoảng 2,3 doanh nghiệp/1.000 dân, đóng góp của kinh tế số khoảng 20,69% GRDP năm 2024, 45 dự án ĐMST được hỗ trợ trong giai đoạn 2020-2025 với tổng 11,4 tỷ đồng, chỉ số ĐMST địa phương đứng thứ 5 cả nước năm 2024. Môi trường ĐMST và kết nối cộng đồng cũng đã hình thành tương đối rõ, thể hiện qua các đầu mối hỗ trợ như DNES, Trung tâm Hỗ trợ khởi nghiệp ĐMST Đà Nẵng, cùng các sự kiện quy mô lớn như DevDay Đà Nẵng, Super Vietnam và Vietnam Blockchain Day.

Trên địa bàn đã xuất hiện một số doanh nghiệp có khả năng tham gia trực tiếp hoặc gián tiếp vào nghiên cứu, thử nghiệm và vận hành các giải pháp liên quan đến blockchain. Trước hết là doanh nghiệp đã tham gia thử nghiệm thực tế như AlphaTrue Solutions với giải pháp BasalPay và Dragon Lab với giải pháp MIMO. Một số doanh nghiệp khác như Kyber Network, Ledger, Figment và HashKey Group cũng đã trao đổi với thành phố về khả năng hiện diện, tuyển dụng, đào tạo kỹ sư blockchain, hỗ trợ khởi nghiệp và thúc đẩy hợp tác công nghệ.

Thành phố cũng bước đầu thiết lập mạng lưới hợp tác với các đối tác công nghệ và thị trường trong nước, quốc tế, thể hiện qua các biên bản ghi nhớ ký với Digital Treasures Centers, Verichains, Bybit Fintech và Abu Dhabi Blockchain Center nhằm thúc đẩy nghiên cứu, ứng dụng và phát triển blockchain. Đồng thời, đã có sự hiện diện của các tổ chức mới trong việc hỗ trợ hệ sinh thái như Hiệp hội Blockchain và Tài sản số Việt Nam, Viện Blockchain và Trí tuệ nhân tạo ABAIL.

Đà Nẵng đã cơ bản hình thành hệ sinh thái blockchain ban đầu với các doanh nghiệp thử nghiệm, các sự kiện cộng đồng và hoạt động hợp tác. Tuy nhiên, số lượng doanh nghiệp công nghệ chuyên sâu về blockchain còn hạn chế, quy mô hoạt động chưa lớn, mức độ liên kết giữa các chủ thể chưa chặt và chuỗi giá trị chưa hoàn chỉnh. Phát triển hệ sinh thái và thu hút thêm doanh nghiệp mới là một trong những nội dung nền tảng cần song hành với quá trình triển khai Đề án.

4. Hiện trạng nguồn nhân lực và năng lực tổ chức thực hiện

Đà Nẵng có nguồn nhân lực công nghệ thông tin khá tốt, với khoảng 53.000 nhân lực công nghệ thông tin, trong đó khoảng 22.000 người làm việc trong lĩnh vực phần mềm và nội dung số; có hệ thống cơ sở đào tạo tương đối phát triển như Đại học Đà Nẵng, Đại học Duy Tân, Đại học FPT. Cùng với môi trường kết nối cộng đồng công nghệ, hội thảo chuyên môn và các sự kiện nghề nghiệp như DevDay, đây là điều kiện

thuận lợi để hình thành, bổ sung và phát triển nguồn nhân lực phục vụ nghiên cứu, tích hợp, vận hành và từng bước mở rộng ứng dụng các công nghệ mới.

Tuy nhiên, cần phân biệt giữa nhân lực công nghệ thông tin nói chung và nhân lực blockchain chuyên sâu. Thành phố hiện có lợi thế về phát triển phần mềm, tích hợp hệ thống và vận hành hạ tầng số, nhưng còn thiếu hụt ở các năng lực chuyên sâu như thiết kế kiến trúc blockchain, quản trị khoá mật mã, kiểm toán bảo mật hợp đồng thông minh (smart contract), ATTT, ANM hệ thống, giám sát rủi ro, quản trị và truy vết dữ liệu trên chuỗi, đặc biệt là đối với thị trường TSMH. Khoảng cách này càng rõ hơn trong khu vực nhà nước, khi kinh nghiệm quản lý và vận hành hệ thống blockchain vẫn đang ở mức cơ bản, chưa hình thành năng lực quản trị và vận hành thường xuyên trên diện rộng.

Có thể đánh giá nguồn nhân lực hiện tại đủ để bắt đầu triển khai theo hướng có chọn lọc và từng bước song hành với đào tạo nâng cao năng lực chuyên môn, bên cạnh xây dựng cơ chế thu hút chuyên gia giỏi trong nước, chuyên gia người Việt Nam ở nước ngoài và đối tác quốc tế, phát triển năng lực theo từng bài toán và trong dài hạn. Hạn chế chính là thiếu hụt nhân lực chuyên sâu có kinh nghiệm vận hành thực tế đối với hệ thống blockchain có yêu cầu cao về kiến trúc, an toàn, quản trị dữ liệu và kiểm soát rủi ro. Đây là một trong những nhiệm vụ quan trọng cần đưa vào Đề án để triển khai trong giai đoạn sắp tới, theo hướng chuyên sâu, gắn với yêu cầu cụ thể.

5. Hiện trạng ứng dụng và thử nghiệm

Thời gian qua, thành phố đã triển khai các ứng dụng thử nghiệm blockchain ban đầu như truy xuất nguồn gốc cho các sản phẩm đặc sản như đá mỹ nghệ Non Nước và Sâm Ngọc Linh; các mô hình tài chính số theo cơ chế sandbox như BasalPay của Công ty cổ phần AlphaTrue Solutions và MIMO của Dragon Lab về chuyển đổi USDT sang đồng Việt Nam qua mô hình trung gian không lưu ký. Các thử nghiệm này giúp thành phố có thêm kinh nghiệm tiếp cận công nghệ, nhận diện yêu cầu tích hợp, yêu cầu giám sát và các vấn đề phát sinh trong thực tiễn triển khai.

Tuy nhiên, các kết quả thử nghiệm hiện nay phạm vi ứng dụng còn hẹp, dữ liệu đánh giá hiệu quả còn ít và các mô hình chưa kết nối với nhau trong một kiến trúc thống nhất. Các hoạt động hiện nay cho thấy nhiều lĩnh vực tại thành phố có nhu cầu ứng dụng blockchain và cần thiết phải tổ chức triển khai ứng dụng blockchain một cách có hệ thống và đồng bộ trong giai đoạn tới.

6. Đánh giá tổng hợp mức độ sẵn sàng

Mức độ sẵn sàng về phát triển blockchain của thành phố được đánh giá theo 06 nội dung, tổng hợp tại Bảng 1.

Mỗi nội dung được đánh giá theo 04 mức: Mức 1 - Chưa sẵn sàng (chưa hình thành điều kiện cơ bản; cần chuẩn bị trước khi triển khai); Mức 2 - Cơ bản sẵn sàng (có nền tảng ban đầu, còn nhiều khoảng trống cần bổ sung trong quá trình thực hiện Đề án); Mức 3 - Sẵn sàng (đã đủ điều kiện triển khai theo lộ trình có chọn lọc, còn dư địa hoàn thiện); Mức 4 - Đồng bộ toàn diện (đã đồng bộ toàn diện, không còn khoảng trống đáng kể, đủ điều kiện triển khai trên diện rộng).

Bảng 1. Bảng đánh giá mức độ sẵn sàng về phát triển blockchain của thành phố

Nội dung đánh giá	Mức	Căn cứ định lượng
1. Thể chế và pháp lý địa phương	3/4	Có cơ chế đặc thù theo Nghị quyết số 136/2024/QH15, Nghị quyết số 259/2025/QH15, Nghị quyết số 55/2024/NQ-HĐND, Quyết định số 3291/QĐ-UBND (Khung kiến trúc số), Quyết định số 3292/QĐ-UBND (Đề án CDS)
2. Hạ tầng số và dữ liệu nền tảng	2/4	Đã có nền tảng tích hợp và chia sẻ dữ liệu, 02 TTDL nhà nước (chính tại Hải Châu, dự phòng tại Tam Kỳ); tuy nhiên mức độ chuẩn hóa dữ liệu giữa các hệ thống nguồn chưa đồng đều, cần tiếp tục chuẩn hóa
3. Nhân lực blockchain chuyên sâu	2/4	22.000 nhân lực phần mềm; nhân lực blockchain chuyên sâu trong cả khu vực công và tư còn hạn chế
4. Hệ sinh thái doanh nghiệp, cơ sở đào tạo	3/4	Có DNES, Hiệp hội Blockchain và Tài sản số Việt Nam, Viện ABAIL; các biên bản ghi nhớ với Digital Treasures, Verichains, Bybit, Abu Dhabi Blockchain Center; số lượng doanh nghiệp blockchain chuyên sâu còn ít
5. Kinh nghiệm thí điểm	3/4	Có thí điểm BasalPay, MIMO; truy xuất nguồn gốc đá Non Nước, Sâm Ngọc Linh; phạm vi hẹp, dữ liệu đánh giá còn ít
6. Năng lực điều phối liên ngành	2/4	Có Sở KH&CN làm đầu mối, có kinh nghiệm điều hành sandbox theo Nghị quyết số 55/2024/NQ-HĐND; thiếu năng lực vận hành blockchain thường xuyên trên diện rộng
Tổng cộng	15/24	Sẵn sàng triển khai có chọn lọc theo lộ trình

IV. NHÓM BÀI TOÁN CẦN GIẢI QUYẾT

1. Nhóm bài toán về dữ liệu tin cậy, xác minh, toàn vẹn và truy vết trong quản lý nhà nước

Đây là nhóm bài toán phát sinh trực tiếp từ quá trình vận hành chính quyền số, dịch vụ công trực tuyến và liên thông dữ liệu ở quy mô ngày càng lớn của thành phố. Khi số lượng hồ sơ điện tử, giao dịch dữ liệu và quy trình liên cơ quan tăng lên, nhu cầu xác định rõ tính toàn vẹn của hồ sơ, truy vết trạng thái xử lý, kiểm chứng độc lập và làm rõ trách nhiệm giữa các bên tham gia trở nên hiện hữu.

Nhóm bài toán này bao gồm các yêu cầu như bảo đảm toàn vẹn hồ sơ điện tử, xác minh văn bản, chứng chỉ, kiểm chứng dữ liệu chuyên ngành và hỗ trợ đối soát trong các quy trình xử lý có nhiều chủ thể tham gia. Với đặc điểm đó, đây là nhóm bài toán có mức độ sẵn sàng triển khai cao nhất, khi gắn trực tiếp với hạ tầng số và dữ liệu mà thành phố đã có, đồng thời có đầu mối quản lý tương đối rõ, làm cơ sở hình thành giá trị sử dụng

thực tế và kiểm chứng tính khả thi của mô hình hạ tầng chuỗi khối dùng chung của thành phố Đà Nẵng.

2. Nhóm bài toán về ứng dụng chuyên ngành có dữ liệu phức tạp, nhạy cảm và điều kiện cao

Nhóm bài toán này phát sinh từ nhu cầu ứng dụng blockchain trong các lĩnh vực có dữ liệu phức tạp, mức độ nhạy cảm cao và yêu cầu chặt chẽ hơn về tích hợp, BVDLCN và tổ chức thực hiện, như bản sao số đô thị, hồ sơ y tế và một số lĩnh vực chuyên ngành khác.

Đây là những bài toán có giá trị thực tiễn và tiềm năng ứng dụng rõ, nhưng điều kiện triển khai cao hơn đáng kể so với nhóm bài toán thứ nhất. Mức độ sẵn sàng hiện nay mới ở mức trung bình, vì còn phụ thuộc vào chất lượng dữ liệu nguồn, chuẩn hoá liên hệ thống, điều kiện pháp lý chuyên ngành, cơ chế BVDLCN và năng lực phối hợp giữa các đơn vị liên quan. Vì vậy, nhóm này phù hợp với cách tiếp cận mở rộng theo điều kiện: phải chuẩn hóa dữ liệu, quy trình, đầu mối và cơ chế bảo vệ trước khi đưa vào triển khai ở quy mô rộng.

3. Nhóm bài toán về kinh tế dữ liệu và dịch vụ số

Nhóm bài toán này gắn với nhu cầu từng bước khai thác blockchain trong các hoạt động tạo giá trị từ dữ liệu và dịch vụ số của thành phố, như giao dịch dữ liệu tin cậy, xác minh tài sản sở hữu trí tuệ và các mô hình dịch vụ dùng chung dựa trên dữ liệu tin cậy.

Đây là nhóm bài toán có tiềm năng phát triển gắn với mục tiêu kinh tế số, ĐMST và phát triển dịch vụ đô thị. Tuy nhiên, hiệu quả triển khai phụ thuộc nhiều vào độ trưởng thành của dữ liệu, khả năng phối hợp giữa cơ quan nhà nước và doanh nghiệp, mức độ sẵn sàng của thị trường và sức hấp thụ của các chủ thể tham gia. Do đó, phù hợp với cấp độ triển khai gắn với phát triển kinh tế dữ liệu và dịch vụ số, đi sau nhóm ưu tiên dùng chung, nhưng vẫn cần được chuẩn bị từ sớm.

4. Nhóm bài toán về mô hình chuyên biệt gắn với tài chính số, TSMH, IFC và sandbox

Nhóm bài toán này gắn với các mô hình chuyên biệt trong lĩnh vực tài chính số, TSMH và giao dịch số, hình thành theo hai cơ chế khác biệt: trong IFC Việt Nam tại Đà Nẵng theo cơ chế riêng của IFC; và trong cơ chế sandbox của thành phố theo Nghị quyết số 55/2024/NQ-HĐND đối với các mô hình đã được cấp Giấy chứng nhận. Đây là nhóm bài toán có bản chất khác biệt, vì không chỉ phụ thuộc vào yếu tố công nghệ và dữ liệu, mà còn chịu tác động trực tiếp của pháp luật chuyên ngành, điều kiện thị trường, năng lực giám sát rủi ro và quyết định của cơ quan có thẩm quyền. Trong nhóm này, thành phố đã có một số thử nghiệm bước đầu, cho thấy nhu cầu và khả năng tiếp cận là có thật.

Tuy nhiên, mức độ rủi ro cao hơn và phạm vi pháp lý chặt hơn so với các nhóm bài toán khác. Vai trò của thành phố cần được xác định đúng trong khuôn khổ quản lý nhà nước, điều phối, kết nối hạ tầng và hỗ trợ giám sát khi phù hợp. Đây không phải nhóm nội dung có thể triển khai theo cùng cơ chế với các ứng dụng dùng chung của thành phố. Tổ chức được cấp phép trong IFC hoặc trong sandbox không tự động được mở rộng phục vụ ngoài phạm vi đã được phê duyệt; mở rộng phải có quyết định của cơ quan có thẩm quyền.

CHƯƠNG III: QUAN ĐIỂM, MỤC TIÊU VÀ NỘI DUNG ĐỀ ÁN

I. QUAN ĐIỂM XÂY DỰNG ĐỀ ÁN

1. Ứng dụng blockchain phục vụ người dân, doanh nghiệp; phát triển chính quyền số và kinh tế dữ liệu

Blockchain là một trong những công nghệ chiến lược quốc gia theo Quyết định số 1131/QĐ-TTg và Quyết định số 21/2026/QĐ-TTg (có hiệu lực kể từ ngày 01/7/2026), là một trong ba trụ cột kinh tế số của thành phố theo Quyết định số 3292/QĐ-UBND, được thành phố ưu tiên triển khai trong giai đoạn 2026-2030 nhằm nâng cao hiệu lực, hiệu quả quản lý nhà nước, chất lượng phục vụ người dân, doanh nghiệp; phát triển chính quyền số, kinh tế số, kinh tế dữ liệu và ĐMST của thành phố.

2. Bám sát bài toán thực tiễn, phù hợp với mức độ sẵn sàng và khả năng tổ chức thực hiện của thành phố

Chỉ lựa chọn triển khai đối với các nội dung mà blockchain thực sự tạo ra giá trị bổ sung rõ rệt so với hệ thống hiện có, nhất là trong các trường hợp có yêu cầu cao về xác minh, kiểm chứng, truy vết, đối soát và chia sẻ dữ liệu tin cậy giữa nhiều chủ thể. Việc triển khai bám sát nhóm bài toán đã xác định, phù hợp với điều kiện dữ liệu, điều kiện pháp lý, khả năng tích hợp, nguồn lực và năng lực tổ chức thực hiện trong từng giai đoạn; không triển khai theo phong trào, không đầu tư dàn trải, không áp dụng đối với các nội dung chưa đủ điều kiện hoặc không tạo ra hiệu quả thực tiễn.

3. Xây dựng hạ tầng chuỗi khối dùng chung của thành phố

Xây dựng và vận hành hạ tầng blockchain dùng chung của thành phố (DNC-Chain) là hạ tầng chuỗi khối lớp 1 có cấp phép (permissioned Layer-1) bảo đảm kết nối, liên thông, đồng bộ và đối soát với Nền tảng chuỗi khối quốc gia theo tiêu chuẩn và hướng dẫn của cơ quan có thẩm quyền để chủ động phục vụ các bài toán đặc thù của thành phố về quản lý nhà nước, kinh tế dữ liệu và dịch vụ số. DNC-Chain không sao chép dữ liệu cốt lõi cấp quốc gia; không xây dựng lại các chức năng lõi đã được triển khai tập trung tại cấp quốc gia.

4. Kết hợp mục tiêu quản lý nhà nước với phát triển hệ sinh thái, huy động sự tham gia của khu vực tư nhân; áp dụng cơ chế đặc thù của thành phố phù hợp phạm vi thẩm quyền

Chính quyền thành phố giữ vai trò kiến tạo, định hướng, điều phối, giám sát và quản lý rủi ro; doanh nghiệp, cơ sở đào tạo, viện nghiên cứu và cộng đồng chuyên gia là lực lượng tham gia nghiên cứu, phát triển, vận hành và mở rộng ứng dụng theo cơ chế phù hợp. Phân định rõ giữa nội dung quản lý nhà nước và nội dung có bản chất thương mại; NSNN chỉ sử dụng cho các nội dung thuộc phạm vi quản lý nhà nước, hạ tầng dùng chung và các điều kiện nền tảng cần thiết. Áp dụng có chọn lọc cơ chế đặc thù theo Nghị quyết số 136/2024/QH15, Nghị quyết số 259/2025/QH15 và các nghị quyết của HĐND thành phố trong phạm vi thẩm quyền.

5. Gắn với định hướng công nghệ chiến lược quốc gia; tuân thủ pháp luật Việt Nam và tiêu chuẩn kỹ thuật quốc tế, trong nước

Đề án gắn với định hướng phát triển công nghệ chiến lược quốc gia theo Quyết định số 1131/QĐ-TTg (được thay thế bởi Quyết định số 21/2026/QĐ-TTg ngày 30/4/2026 kể từ ngày 01/7/2026) và Quyết định số 2815/QĐ-TTg; thành phố vừa là đơn vị ứng dụng, vừa từng bước làm chủ công nghệ blockchain; ưu tiên nền tảng có công nghệ lõi do doanh nghiệp, tổ chức Việt Nam phát triển. DNC-Chain tuân thủ đồng thời các quy định pháp luật Việt Nam và các tiêu chuẩn kỹ thuật quốc tế, trong nước có liên quan; không phát sinh tiêu chuẩn riêng, không tạo ốc đảo công nghệ.

6. Bảo đảm ATTT, ANM, BVDLCN và quản trị rủi ro xuyên suốt vòng đời

ATTT, ANM, BVDLCN và quản trị rủi ro được tích hợp ngay từ giai đoạn thiết kế chính sách và xuyên suốt toàn bộ vòng đời của hạ tầng và ứng dụng. Thành phố phối hợp chặt chẽ với các cơ quan có thẩm quyền trong giám sát, kiểm định và xử lý các yêu cầu can thiệp khẩn cấp đối với các mô hình có yếu tố tài chính số, TSMH và giao dịch số; bảo đảm an toàn cho người dùng và phòng, chống lừa đảo, lạm dụng công nghệ.

7. Phát triển đồng bộ nguồn nhân lực, hệ sinh thái và đổi mới sáng tạo

Phát triển đồng bộ nguồn nhân lực, hệ sinh thái doanh nghiệp, viện nghiên cứu, cơ sở đào tạo và cộng đồng chuyên gia để bảo đảm năng lực triển khai, vận hành và mở rộng các ứng dụng blockchain; triển khai cơ chế thành phố là khách hàng đầu tiên theo Quyết định số 2815/QĐ-TTg và đặt hàng nghiên cứu cấp thành phố; thúc đẩy hợp tác quốc tế, chuyển giao công nghệ.

II. NGUYÊN TẮC TRIỂN KHAI

1. Dữ liệu nghiệp vụ được quản lý tại hệ thống nguồn; blockchain chỉ ghi nhận lớp tin cậy số cần thiết

Dữ liệu nghiệp vụ và dữ liệu chuyên ngành (bao gồm dữ liệu cá nhân) tiếp tục được tạo lập, lưu trữ và quản lý tại các hệ thống nguồn theo đúng chức năng, thẩm quyền, phù hợp pháp luật về giao dịch điện tử, dữ liệu, BVDLCN và quy định chuyên ngành. Blockchain không thay thế cơ sở dữ liệu, hệ thống thông tin nghiệp vụ và nền tảng tích hợp, chia sẻ dữ liệu của thành phố; chỉ ghi nhận bằng chứng xác minh, dữ liệu tham chiếu và dữ liệu tối thiểu để phục vụ kiểm chứng, đối soát, truy vết, hậu kiểm; tuân thủ nguyên tắc tối thiểu hoá dữ liệu, đặc biệt với dữ liệu nhạy cảm, y tế, giáo dục và chuyên ngành đặc thù.

Định danh cá nhân trong các ứng dụng triển khai trên DNC-Chain sử dụng trực tiếp VNeID, CSDL quốc gia về dân cư và tiêu chuẩn của Bộ Công an; không xây dựng hệ thống định danh công dân song song. Định danh tổ chức, doanh nghiệp, thiết bị, hàng hoá, tài sản áp dụng TCVN/QCVN và quy định chuyên ngành.

2. Triển khai theo kiến trúc thống nhất, tích hợp và liên thông có kiểm soát

Việc triển khai bám sát Khung kiến trúc số thành phố Đà Nẵng và định hướng Nền tảng chuỗi khối quốc gia; không phát sinh phân mảnh kiến trúc, chồng chéo chức năng hay xung đột với các nền tảng dùng chung hiện có. DNC-Chain được thiết kế theo tiêu

chuẩn kiến trúc mạng kế thừa nguyên vẹn lớp đồng thuận, lớp xác thực, lớp quản trị khoá và lớp giám sát của nền tảng layer-1 được cơ quan có thẩm quyền thẩm định và công nhận; bảo đảm khả năng liên thông, không tạo thiết kế tách biệt với Nền tảng chuỗi khối quốc gia khi được ban hành chính thức, theo nguyên tắc tận dụng tối đa hạ tầng dùng chung cấp quốc gia, không đầu tư lại các chức năng lõi đã được xác định xây dựng tập trung cấp quốc gia.

Về khung tiêu chuẩn áp dụng, DNC-Chain và các ứng dụng kết nối tuân thủ đồng thời các tiêu chuẩn quốc tế chuyên ngành chuỗi khối, các tiêu chuẩn quốc tế chung về mật mã và an toàn thông tin; Khung kiến trúc Chính phủ số, kiến trúc tổng thể quốc gia số, kiến trúc dữ liệu quốc gia, khung kiến trúc số của thành phố; danh mục TCVN/QCVN do cơ quan có thẩm quyền ban hành; trong đó có TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ; định kỳ rà soát, cập nhật theo lộ trình hoàn thiện khung tiêu chuẩn quốc gia.

Về cơ chế liên thông có kiểm soát: (i) kết nối, liên thông với nền tảng chuỗi khối quốc gia theo tiêu chuẩn và hướng dẫn của cơ quan có thẩm quyền (mặc định); (ii) liên thông với các nền tảng chuỗi khối khác có điều kiện, qua Cầu nối Đa chuỗi với danh sách điểm tin cậy (allowlist) do cơ quan chủ trì cấp phép; DNC-Chain không kết nối trực tiếp với nền tảng chuỗi khối bên ngoài nếu không qua cổng kiểm soát, bảo đảm quyền chủ động quản trị và dữ liệu của thành phố.

3. Triển khai theo cấp độ, gắn với điều kiện và phạm vi thẩm quyền

Đề án thực hiện theo lộ trình phù hợp với mức độ sẵn sàng của từng nhóm ứng dụng, hệ thống và điều kiện về dữ liệu, pháp lý, kỹ thuật, nguồn lực và tổ chức thực hiện. Danh mục sản phẩm được phân thành 04 tầng theo bản chất, mức độ sẵn sàng và cơ chế áp dụng; mỗi sản phẩm được quản lý theo 04 mốc: chuẩn bị, kiểm thử, bắt đầu vận hành và mở rộng có điều kiện. Mốc kiểm thử được thực hiện trên dữ liệu thật, có cơ quan chủ trì xác định bằng văn bản; việc chuyển mốc chỉ thực hiện trên cơ sở đánh giá kết quả thực tế, mức độ đáp ứng các điều kiện đã xác lập và quyết định bằng văn bản của cơ quan có thẩm quyền. Không áp dụng cùng một cơ chế triển khai cho mọi nhóm sản phẩm.

4. Bảo đảm tuân thủ pháp luật, an toàn, an ninh, bảo vệ dữ liệu và quản trị rủi ro trong toàn bộ quá trình triển khai

Mọi nội dung triển khai phù hợp với chủ trương của Đảng, pháp luật của Nhà nước, cơ chế đặc thù của thành phố và quy định chuyên ngành. Quản trị rủi ro bao quát bốn nhóm: rủi ro kỹ thuật (hạ tầng, dữ liệu, ứng dụng); rủi ro tài chính và tuân thủ đối với các mô hình tài chính số gắn với cơ sở IFC tại Đà Nẵng và sandbox của thành phố; rủi ro xã hội (bảo vệ người dùng, phòng chống lừa đảo, lạm dụng công nghệ huy động vốn trái phép); rủi ro uy tín.

Đối với các mô hình có yếu tố tài sản mã hoá, giao dịch số và gọi vốn cộng đồng, việc triển khai phải tích hợp cơ chế xác minh danh tính điện tử; phòng, chống rửa tiền, chống tài trợ khủng bố, chống tài trợ phổ biến vũ khí hủy diệt hàng loạt (AML/CFT/CTTPBVKHDHL) theo Nghị định số 329/2025/NĐ-CP; tuân thủ Khuyến nghị FATF (bao gồm Quy tắc Travel Rule); lưu vết giao dịch, giám sát bất thường; báo cáo và cung cấp thông tin cho cơ quan có thẩm quyền.

5. Phân loại nội dung quản lý nhà nước, nội dung doanh nghiệp tham gia và nội dung thực hiện theo cơ chế riêng

Đề án phân định ba phạm vi thực hiện: (i) nội dung thuộc trách nhiệm quản lý của cơ quan nhà nước; (ii) nội dung doanh nghiệp tham gia nghiên cứu, phát triển, cung cấp dịch vụ và vận hành theo cơ chế đặt hàng hoặc hợp tác; (iii) nội dung thực hiện theo cơ chế riêng - áp dụng sandbox của thành phố trong phạm vi không gian theo Khoản 1 Điều 1 Nghị quyết số 55/2024/NQ-HĐND. Đối với các mô hình có bản chất thương mại, Đề án chỉ thực hiện vai trò tiếp nhận, điều phối, tích hợp và hỗ trợ quản trị rủi ro trong phạm vi chức năng quản lý nhà nước; phân định rõ giữa phần quản lý nhà nước với phần đầu tư, vận hành thương mại của doanh nghiệp.

III. MỤC TIÊU CỦA ĐỀ ÁN

1. Mục tiêu tổng quát

Hình thành hạ tầng blockchain dùng chung của thành phố mang tên DNC-Chain, đóng vai trò lớp tin cậy số trong kiến trúc hạ tầng số, phát triển theo hướng mở, có khả năng tích hợp, mở rộng và liên thông. Từng bước triển khai các ứng dụng blockchain phù hợp theo thứ tự ưu tiên, điều kiện và phạm vi thẩm quyền nhằm phục vụ chính quyền số, quản lý dữ liệu tin cậy và phát triển kinh tế dữ liệu.

Phát triển đồng bộ nguồn nhân lực, hệ sinh thái và cơ chế tham gia của khu vực tư nhân để bảo đảm khả năng triển khai, vận hành và mở rộng các ứng dụng blockchain trong giai đoạn 2026-2030; góp phần nâng cao hiệu quả quản lý nhà nước, tăng độ tin cậy của dữ liệu số, thúc đẩy ĐMST và tạo thêm động lực phát triển kinh tế số của thành phố.

2. Mục tiêu cụ thể đến năm 2030

a) Về thể chế, quản trị và tiêu chuẩn triển khai

- Hoàn thiện rà soát, hệ thống hóa khung pháp lý áp dụng cho triển khai Đề án;
- Hoàn thiện Quy chế quản trị, vận hành và khai thác hạ tầng blockchain dùng chung của thành phố;
- Hoàn thiện Quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời ứng dụng trên hạ tầng blockchain dùng chung;
- Hoàn thiện Bộ tiêu chuẩn, yêu cầu kết nối, chia sẻ và kiểm chứng dữ liệu áp dụng đối với các hệ thống kết nối với hạ tầng blockchain dùng chung, bám sát danh mục TCVN/QCVN về công nghệ blockchain, nền tảng dữ liệu, ATTT, ANM, cùng các văn bản hướng dẫn có liên quan;
- Hoàn thiện Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án;
- Hoàn thiện Quy chế bảo đảm ATTT, ANM và BVDLCN đối với DNC-Chain và các ứng dụng kết nối.

b) Về hạ tầng, nền tảng và kết nối kỹ thuật

- Xây dựng và đưa vào vận hành 01 hạ tầng blockchain dùng chung của thành phố

mang tên DNC-Chain; ưu tiên nền tảng Layer-1 có công nghệ lõi do doanh nghiệp, tổ chức Việt Nam phát triển, phù hợp với định hướng kiến trúc cấp quốc gia; kết nối, đồng bộ và liên thông với Nền tảng chuỗi khối quốc gia.

- Hoàn thành triển khai 07 mô đun nền tảng dùng chung của DNC-Chain, gồm: Cầu nối Đa chuỗi; Tích hợp, tạo bằng chứng xác minh và đối soát hồ sơ điện tử; Quản lý khoá và phân quyền; Quản lý giao dịch và token; Quản lý smart contract; Quản lý ứng dụng và marketplace; Hub làm sạch dữ liệu;

- Hoàn thành kết nối kỹ thuật giữa DNC-Chain với nền tảng tích hợp, chia sẻ dữ liệu của thành phố và các hệ thống ưu tiên;

- Bảo đảm DNC-Chain được vận hành ổn định, có khả năng tích hợp, giám sát, dự phòng, mở rộng và đáp ứng yêu cầu triển khai các ứng dụng trong phạm vi Đề án.

c) Về triển khai ứng dụng

- Triển khai các sản phẩm ứng dụng ưu tiên gồm: SP1 - Hệ thống bảo đảm toàn vẹn hồ sơ điện tử trên blockchain; SP2 - Hệ thống xác minh văn bằng, chứng chỉ trên blockchain;

- Chuẩn bị điều kiện và từng bước triển khai các sản phẩm gồm: SP3 - Bản sao số đô thị (Digital Twin) tích hợp blockchain và SP4 - Hệ thống xác minh hồ sơ y tế trên blockchain khi đáp ứng yêu cầu về dữ liệu, pháp lý và tổ chức thực hiện;

- Triển khai các sản phẩm thuộc nhóm kinh tế dữ liệu và dịch vụ số tích hợp blockchain gồm: SP5 - Sàn giao dịch dữ liệu thành phố; SP6 - Sàn giao dịch tài sản sở hữu trí tuệ; SP7 - Chương trình khách hàng trung thành của thành phố (City Loyalty Program), trên cơ sở bảo đảm điều kiện về dữ liệu, phối hợp và thị trường;

- Tiếp tục theo dõi, đánh giá và chuẩn bị điều kiện mở rộng phạm vi thí điểm đối với SP8 theo cơ chế thử nghiệm có kiểm soát (sandbox) của thành phố; điều phối và chuẩn bị điều kiện triển khai đối với SP9 và SP10 theo cơ chế của IFC Việt Nam tại Đà Nẵng;

- Đến năm 2030, toàn bộ 10 sản phẩm của Đề án (SP1 đến SP10) được triển khai, mở rộng hoặc thuộc phạm vi điều phối theo đúng cấp độ, điều kiện và cơ chế áp dụng của từng nhóm sản phẩm.

d) Về dữ liệu, tích hợp, an toàn, an ninh và bảo vệ dữ liệu

- Chuẩn hoá và sẵn sàng dữ liệu nguồn đối với các hệ thống phục vụ triển khai ứng dụng ưu tiên trong giai đoạn 2026-2027, bám sát Khung kiến trúc dữ liệu quốc gia và Danh mục dữ liệu quan trọng, dữ liệu cốt lõi;

- Từng bước mở rộng phạm vi chuẩn hoá đối với dữ liệu phục vụ các ứng dụng mở rộng và ứng dụng kinh tế dữ liệu trong giai đoạn 2028-2030;

- Thiết lập cơ chế bảo đảm chất lượng, đối soát và xử lý sai lệch dữ liệu trong tích hợp giữa hệ thống nguồn, nền tảng tích hợp, chia sẻ dữ liệu của thành phố và DNC-Chain;

- Bảo đảm các yêu cầu về ATTT, ANM, quản lý truy cập, lưu vết, giám sát vận hành và BVDLCN trong toàn bộ quá trình triển khai, phù hợp với Luật Giao dịch điện tử, Luật Dữ liệu, Luật BVDLCN và các quy định chuyên ngành có liên quan;

- Thiết lập cơ chế kiểm tra, đánh giá, kiểm soát tuân thủ và xử lý sự cố đối với hạ tầng và ứng dụng thành phần.

đ) Về nguồn nhân lực, hệ sinh thái và đổi mới sáng tạo

- Đưa nội dung blockchain vào chương trình đào tạo của các cơ sở giáo dục đại học, cao đẳng trên địa bàn thành phố phù hợp với điều kiện thực tế;

- Tổ chức đào tạo, bồi dưỡng đội ngũ nhân lực phục vụ quản trị, vận hành, tích hợp, kiểm thử, giám sát an toàn và phát triển ứng dụng trên hạ tầng DNC-Chain;

- Hoàn thiện Khung năng lực vận hành hệ thống blockchain thành phố làm căn cứ đào tạo, tuyển dụng và bố trí nhân lực;

- Phân đầu đến năm 2030 có tối thiểu 1.000 nhân lực có kiến thức và kỹ năng liên quan đến blockchain trên địa bàn thành phố; hình thành đội ngũ chuyên gia nòng cốt về thiết kế kiến trúc blockchain, quản trị khoá mật mã và kiểm toán bảo mật smart contract;

- Hình thành hệ sinh thái doanh nghiệp, viện nghiên cứu, cơ sở đào tạo và tổ chức hỗ trợ tham gia nghiên cứu, phát triển, thử nghiệm, cung cấp sản phẩm và dịch vụ trên nền tảng DNC-Chain;

- Triển khai có hiệu quả cơ chế thành phố là khách hàng đầu tiên đối với sản phẩm blockchain theo Quyết định số 2815/QĐ-TTg của Thủ tướng Chính phủ;

- Tổ chức thực hiện đặt hàng nhiệm vụ nghiên cứu, phát triển ứng dụng blockchain cấp thành phố, gắn với Chương trình công nghệ chiến lược quốc gia;

- Thúc đẩy hợp tác quốc tế, chuyển giao công nghệ và thu hút chuyên gia blockchain phục vụ triển khai Đề án;

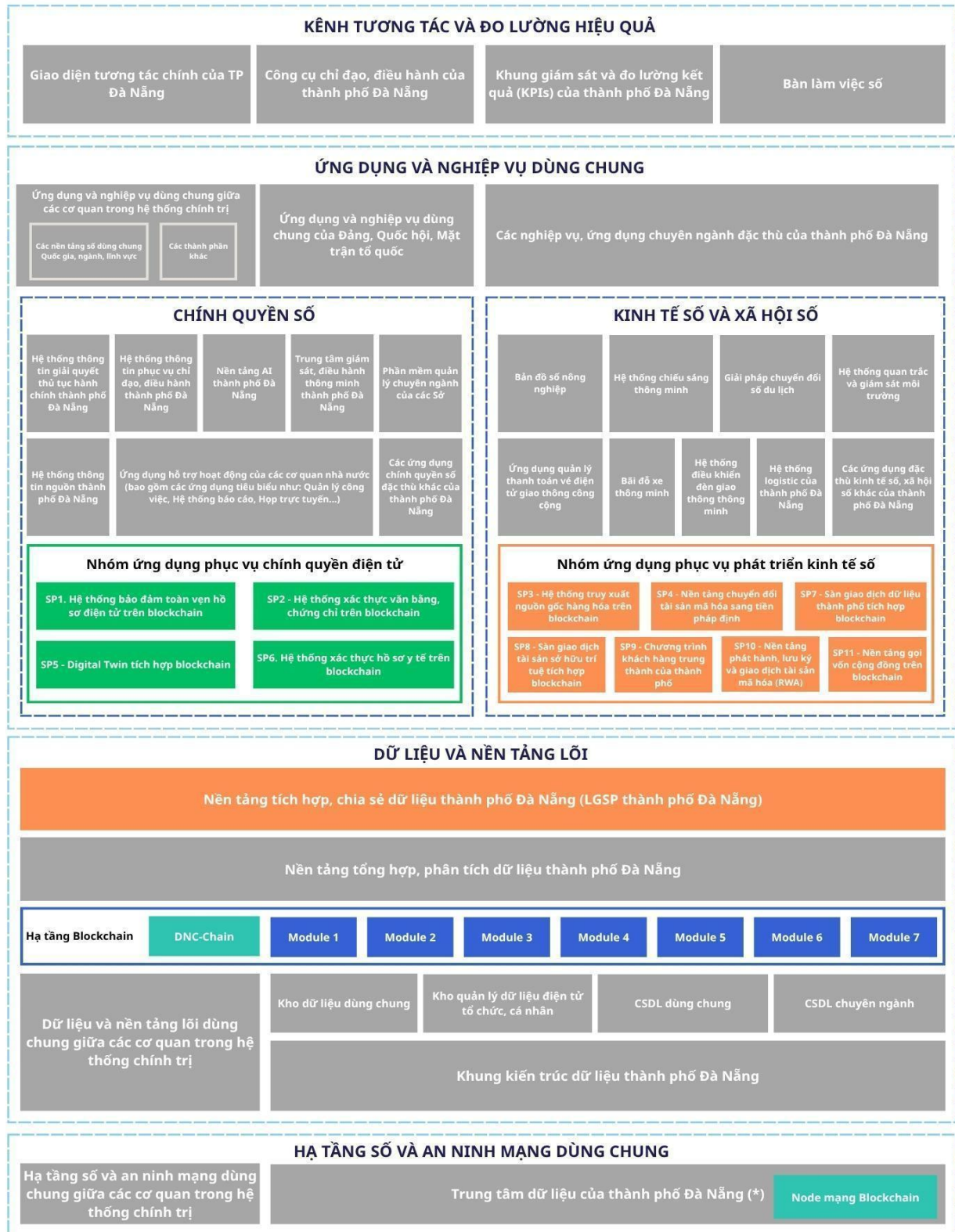
- Phân đầu đến năm 2030 có tối thiểu 30 doanh nghiệp tham gia phát triển hoặc cung cấp giải pháp, sản phẩm, dịch vụ liên quan đến blockchain trên địa bàn và triển khai tối thiểu 08 nhiệm vụ đặt hàng nghiên cứu cấp thành phố về blockchain gắn với nhu cầu thực tiễn.

IV. MÔ HÌNH MẠNG BLOCKCHAIN ĐÀ NẴNG

1. Mô hình mạng blockchain trong khung kiến trúc số thành phố

Mô hình mạng blockchain Đà Nẵng trong Khung kiến trúc số của thành phố bao gồm hạ tầng blockchain và các ứng dụng sử dụng công nghệ blockchain, thuộc Lớp dữ liệu và nền tảng lõi và Lớp ứng dụng và nghiệp vụ dùng chung, được thể hiện tại Hình 1.

KHUNG KIẾN TRÚC SỐ THÀNH PHỐ ĐÀ NẴNG



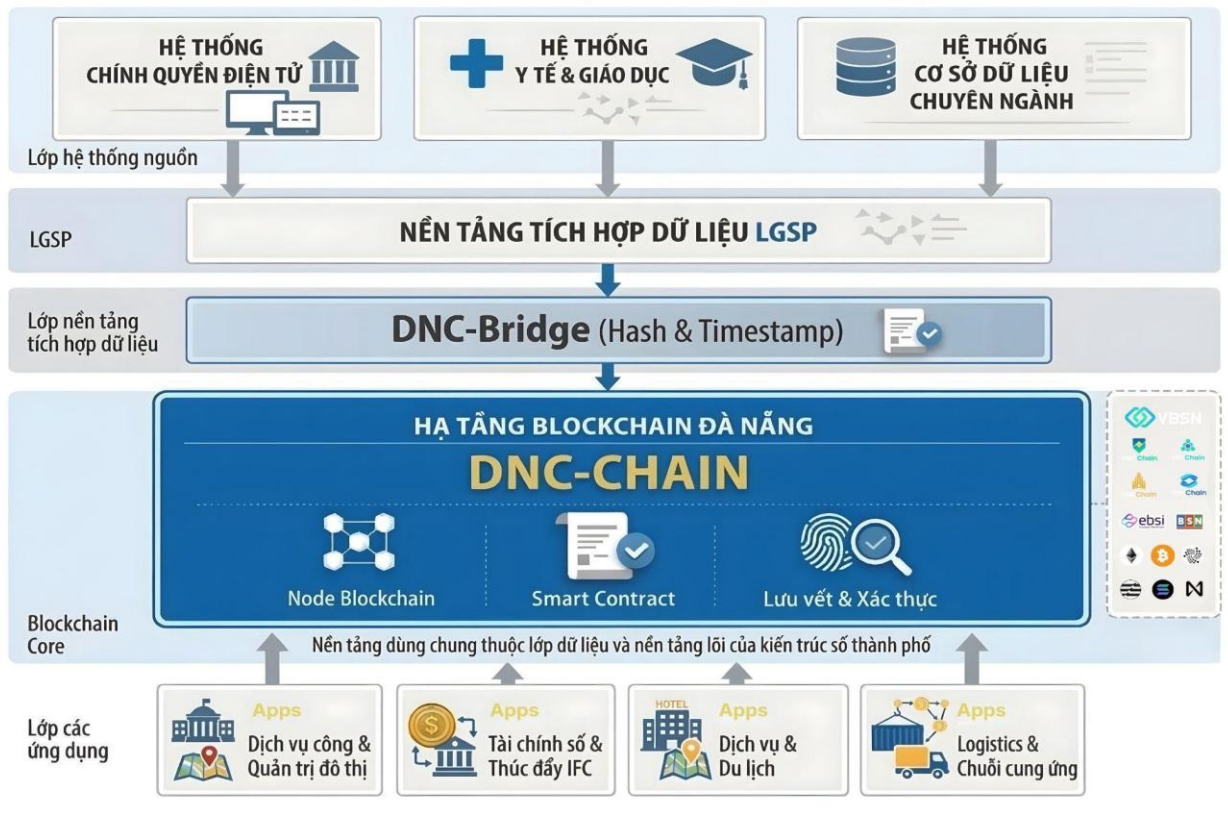
Hình 1. Mô hình mạng blockchain trong Khung kiến trúc số thành phố Đà Nẵng

DNC-Chain giữ vai trò lớp tin cậy số phục vụ các bài toán xác minh, kiểm chứng, truy vết, đối soát và khai thác dữ liệu tin cậy. Trên DNC-Chain, thành phố triển khai các ứng dụng thành phần gắn với ba nhóm chức năng chính: xác minh và kiểm chứng dữ liệu phục vụ quản lý nhà nước; truy vết và quản lý chuỗi dữ liệu phục vụ quản lý chất lượng, quản lý đô thị và phát triển kinh tế dữ liệu; theo dõi, giám sát các giao dịch tài chính số và hoạt động thương mại trong phạm vi được phép.

2. Kiến trúc DNC-Chain khi tích hợp vào các hệ thống nguồn hiện có

Về kiến trúc kỹ thuật, DNC-Chain tổ chức theo mô hình mạng có cấp phép, bảo đảm kiểm soát thành viên tham gia, quyền vận hành node, quyền xác minh, quyền thay đổi cấu hình và kết nối liên thông. Phân định rõ trách nhiệm giữa cơ quan quản trị mạng, đơn vị vận hành hạ tầng, đơn vị chủ trì ứng dụng và các chủ thể tích hợp. DNC-Chain bổ sung lớp tin cậy số dùng chung để ghi nhận bằng chứng xác minh, hỗ trợ kiểm chứng độc lập, truy vết và đối soát trong các quy trình có nhiều chủ thể tham gia. Mô hình tích hợp và liên thông được thể hiện tại Hình 2 và qua 05 lớp kiến trúc tại Bảng 2.

Các hệ thống nguồn tiếp tục là nơi tạo lập, cập nhật, lưu trữ và quản lý dữ liệu nghiệp vụ theo đúng chức năng và thẩm quyền của từng cơ quan, đơn vị. Nền tảng tích hợp và chia sẻ dữ liệu của thành phố (LGSP) giữ vai trò kết nối, điều phối và chia sẻ dữ liệu giữa các hệ thống; DNC-Chain chỉ ghi nhận bằng chứng xác minh và lưu vết kỹ thuật theo phạm vi được cấp quyền thông qua Mô đun tích hợp của DNC-Chain.



Hình 2. Mô hình kiến trúc tích hợp DNC-Chain với các hệ thống nguồn hiện có

Bảng 2. Các lớp kiến trúc trong Khung kiến trúc số thành phố

Lớp kiến trúc	Vai trò chính
1. Hệ thống nguồn và cơ sở dữ liệu	Tạo lập, cập nhật, lưu trữ và quản lý dữ liệu nghiệp vụ gốc của các cơ quan, đơn vị, lĩnh vực chuyên ngành; là nơi chịu trách nhiệm nghiệp vụ và pháp lý đối với dữ liệu.
2. Lớp tích hợp và chia sẻ dữ liệu	Kết nối, điều phối và chia sẻ dữ liệu giữa các hệ thống thông qua nền tảng tích hợp, chia sẻ dữ liệu của thành phố (LGSP) và các thành phần trung gian tích hợp.
3. Lớp dữ liệu và nền tảng lõi	Cung cấp các nền tảng lõi dùng chung; trong đó DNC-Chain giữ vai trò lớp tin cậy số, cùng các mô đun nền tảng, công cụ xử lý và phân tích dữ liệu.
4. Lớp ứng dụng và nghiệp vụ dùng chung	Các sản phẩm và dịch vụ khai thác DNC-Chain phục vụ chính quyền số, kinh tế số, xã hội số và các lĩnh vực chuyên ngành.
5. Lớp kênh tương tác, điều hành và đo lường hiệu quả	Các giao diện tương tác, công cụ chỉ đạo, điều hành, giám sát, đo lường kết quả và các kênh phục vụ theo dõi, đánh giá hiệu quả hoạt động của toàn bộ hệ thống.

Mô hình trên khẳng định ba nguyên tắc cốt lõi: (i) dữ liệu nghiệp vụ gốc tiếp tục được quản lý tại hệ thống nguồn; (ii) mọi trao đổi dữ liệu với DNC-Chain được thực hiện qua lớp tích hợp và chia sẻ dữ liệu của thành phố; (iii) DNC-Chain được đặt đúng vai trò là thành phần thuộc Lớp dữ liệu và nền tảng lõi, cung cấp lớp tin cậy số dùng chung. Thuyết minh kỹ thuật chi tiết DNC-Chain tại Phụ lục I Phần A.

3. Mô hình triển khai ứng dụng trên DNC-Chain

Các ứng dụng triển khai trên DNC-Chain tuân thủ các nguyên tắc kiến trúc nêu trên. Căn cứ tính chất ứng dụng, mức độ sẵn sàng thực tế và cơ chế áp dụng, các sản phẩm được phân thành 04 tầng cấp độ để xác định vai trò của DNC-Chain, điều kiện triển khai, chỉ tiêu đánh giá và trách nhiệm chủ trì đối với từng nhóm sản phẩm.

Bảng 3. Phân tầng cấp độ triển khai sản phẩm

Tầng	Nhóm bài toán	Sản phẩm	Điều kiện / Cơ chế triển khai chủ yếu	Định hướng triển khai
Tầng 1. Ứng dụng ưu tiên triển khai sớm	Dữ liệu tin cậy, xác minh, toàn vẹn và truy vết trong quản lý nhà nước	SP1 - Hệ thống bảo đảm toàn vẹn hồ sơ điện tử trên blockchain; SP2 - Hệ thống xác minh văn bằng, chứng chỉ trên blockchain	Dữ liệu nguồn cơ bản đã có hoặc có thể chuẩn hoá; đầu mối chủ trì sản phẩm và dữ liệu nguồn xác định; hạ tầng DNC-Chain sẵn sàng; khung quản trị và tiêu chuẩn tích hợp đã ban hành	Ưu tiên triển khai trước, tạo kết quả sớm và kiểm chứng mô hình

Tầng	Nhóm bài toán	Sản phẩm	Điều kiện / Cơ chế triển khai chủ yếu	Định hướng triển khai
Tầng 2. Ứng dụng mở rộng theo điều kiện	Ứng dụng chuyên ngành có dữ liệu phức tạp, nhạy cảm và điều kiện cao	SP3 - Bản sao số đô thị (Digital Twin) tích hợp blockchain; SP4 - Hệ thống xác minh hồ sơ y tế trên blockchain	Dữ liệu nguồn phải được chuẩn hoá; yêu cầu pháp lý chuyên ngành được rà soát; cơ chế phối hợp liên ngành được xác lập; hạ tầng DNC-Chain đáp ứng yêu cầu mở rộng	Triển khai khi đủ điều kiện, theo lộ trình phù hợp
Tầng 3. Ứng dụng kinh tế dữ liệu và dịch vụ số	Kinh tế dữ liệu và dịch vụ số	SP5 - Sàn giao dịch dữ liệu thành phố tích hợp blockchain; SP6 - Sàn giao dịch tài sản sở hữu trí tuệ tích hợp blockchain; SP7 - Chương trình khách hàng trung thành của thành phố (City Loyalty Program) tích hợp blockchain	Hạ tầng DNC-Chain vận hành ổn định; khung quản trị dữ liệu và cơ chế tham gia của doanh nghiệp được hoàn thiện; dữ liệu nguồn đạt mức chuẩn hoá; điều kiện pháp lý liên quan được rà soát	Triển khai gắn với phát triển dữ liệu, dịch vụ số và hệ sinh thái
Tầng 4. Mô hình thực hiện theo cơ chế riêng	Mô hình chuyên biệt gắn với tài chính số, TSMH, IFC và cơ chế sandbox	SP8 - Nền tảng chuyên đổi TSMH sang tiền pháp định; SP9 - Nền tảng phát hành, lưu ký và giao dịch TSMH (RWA); SP10 - Nền tảng gọi vốn cộng đồng trên blockchain	Theo quy định tại Khoản 5 Mục II Chương này, áp riêng cho SP8, SP9, SP10	Triển khai theo cơ chế riêng, trong phạm vi điều phối và quản lý nhà nước của thành phố

Trên cơ sở phân tầng tại Bảng 3, vai trò của DNC-Chain được phân định theo từng tầng ứng dụng như sau:

- Đối với Tầng 1: DNC-Chain là hạ tầng blockchain chính, trực tiếp phục vụ các chức năng xác minh, kiểm chứng, truy vết, đối soát và lưu vết đối với các ứng dụng ưu tiên của thành phố. DNC-Chain hỗ trợ tăng độ tin cậy của hồ sơ, chứng nhận, dữ liệu và các quy trình có nhiều chủ thể tham gia; dữ liệu gốc vẫn do hệ thống nguồn quản lý theo chức năng và thẩm quyền.

- Đối với Tầng 2: DNC-Chain tiếp tục là hạ tầng blockchain chính, nhưng điều kiện áp dụng chặt chẽ hơn do đặc điểm của các ứng dụng chuyên ngành có dữ liệu phức tạp, nhạy cảm và yêu cầu cao về tích hợp, pháp lý và bảo vệ dữ liệu. DNC-Chain chỉ ghi nhận lớp tin cậy số cần thiết khi ứng dụng đáp ứng đủ điều kiện đầu vào và không thay thế chức năng quản lý chuyên ngành của cơ quan chủ trì.

- Đối với Tầng 3: DNC-Chain là hạ tầng blockchain chính hoặc hạ tầng kiểm chứng và tích hợp, tùy theo tính chất của từng ứng dụng. DNC-Chain phục vụ xác minh dữ liệu, kiểm chứng trạng thái giao dịch, lưu dấu thời gian và ghi nhận các sự kiện cần kiểm

chứng; không đồng nhất với toàn bộ nền tảng dịch vụ hoặc thị trường giao dịch mà các ứng dụng này vận hành.

- Đối với Tầng 4: DNC-Chain không phải là nền tảng triển khai trực tiếp các sản phẩm Tầng 4; chỉ tham gia khi có yêu cầu của cơ quan có thẩm quyền hoặc khi cần thiết cho mục đích giám sát, đối soát, kiểm chứng, ghi nhận bằng chứng tuân thủ. Khi tham gia, DNC-Chain đóng vai trò hạ tầng kỹ thuật dùng chung, hỗ trợ xác minh, kiểm chứng, tích hợp và kiểm soát rủi ro kỹ thuật; chỉ ghi nhận lớp giám sát, đối soát, cảnh báo, mã tham chiếu, bằng chứng tuân thủ; không tiếp nhận chi tiết giao dịch cá nhân, số dư, dữ liệu người dùng; không phải nền tảng giao dịch chính. Phần triển khai trực tiếp các sản phẩm thuộc Tầng 4 do doanh nghiệp cung cấp dịch vụ thực hiện theo cơ chế riêng (sandbox đối với SP8; cơ chế IFC đối với SP9, SP10) và pháp luật chuyên ngành; sự tham gia của DNC-Chain chỉ thực hiện trong phạm vi điều phối, hỗ trợ quản lý nhà nước và phối hợp của thành phố.

V. NỘI DUNG TRIỂN KHAI ĐỀ ÁN

Các nội dung của Đề án được thực hiện theo 02 giai đoạn: Giai đoạn 2026-2027 tập trung xây dựng hạ tầng DNC-Chain, hoàn thiện điều kiện nền tảng và triển khai các ứng dụng ưu tiên để kiểm chứng tính khả thi của mô hình. Giai đoạn 2028-2030 tập trung mở rộng có điều kiện các ứng dụng kinh tế dữ liệu, dịch vụ số và điều phối triển khai các mô hình thuộc cơ chế riêng gắn với cơ sở IFC tại Đà Nẵng và sandbox theo lộ trình phù hợp. Cụ thể nội dung và lộ trình triển khai theo từng nhóm như sau:

1. Hoàn thiện thể chế, quản trị và tiêu chuẩn triển khai

Thành phố tổ chức rà soát, hệ thống hóa khung pháp lý áp dụng cho Đề án; ban hành đồng bộ các VBQPPL và văn bản hướng dẫn về quản trị, vận hành, tiêu chuẩn kỹ thuật, phối hợp liên ngành và bảo đảm ATTT làm cơ sở triển khai hạ tầng và các ứng dụng. Nội dung bảo đảm tính khả thi, phù hợp thẩm quyền của thành phố và gắn với tiến độ đưa hạ tầng DNC-Chain và các sản phẩm ứng dụng vào vận hành.

Trong giai đoạn 2026-2027, hoàn thành rà soát, hệ thống hóa khung pháp lý và ban hành các văn bản trong nhóm thể chế gồm: Quy chế quản trị, vận hành DNC-Chain; Quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời ứng dụng; Bộ tiêu chuẩn, yêu cầu kết nối, chia sẻ và kiểm chứng dữ liệu; Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc; Quy chế bảo đảm ATTT, ANM và BVDLCN đối với DNC-Chain và các ứng dụng kết nối.

Trong giai đoạn 2028-2030, tổ chức đánh giá việc thực hiện, cập nhật, sửa đổi, bổ sung các văn bản đã ban hành cho phù hợp với thực tiễn triển khai, kết quả rà soát và các văn bản mới của Trung ương; mở rộng phạm vi áp dụng đối với các ứng dụng và nhóm dữ liệu được triển khai theo lộ trình; chủ động kiến nghị đối với các vấn đề pháp lý vượt thẩm quyền hoặc chưa có quy định rõ ở cấp Trung ương.

2. Xây dựng, tổ chức và vận hành hạ tầng DNC-Chain

Thành phố xây dựng hạ tầng blockchain dùng chung DNC-Chain theo mô hình có cấp phép, tương thích các tiêu chuẩn quốc tế phổ biến về smart contract; lựa chọn nền tảng công nghệ Layer-1 theo nguyên tắc kiến trúc tại Khoản 2 Mục II Chương này, trên

cơ sở ưu tiên nền tảng có công nghệ lõi do doanh nghiệp, tổ chức Việt Nam làm chủ khi đáp ứng yêu cầu kỹ thuật, quản trị, an toàn và tích hợp. Hạ tầng được tổ chức phân tán, có khả năng tích hợp, giám sát, dự phòng và mở rộng; bảo đảm mật bằng kỹ thuật thống nhất phục vụ triển khai các ứng dụng của Đề án.

Trong giai đoạn 2026-2027, hoàn thành lựa chọn nền tảng công nghệ Layer-1; thiết lập cấu hình node tối thiểu gồm 01 node quản trị mạng, 01 validator node và 02 node hỗ trợ kỹ thuật tại ít nhất 03 địa điểm độc lập; triển khai 07 mô đun nền tảng dùng chung; hoàn thành kết nối kỹ thuật giữa DNC-Chain với nền tảng tích hợp, chia sẻ dữ liệu của thành phố (LGSP) và các hệ thống nguồn ưu tiên phục vụ các sản phẩm Tầng 1; đưa DNC-Chain vào vận hành ổn định.

Trong giai đoạn 2028-2030, mở rộng cấu hình lên 02 node quản trị mạng, 02 validator node và 02 node hỗ trợ kỹ thuật; tăng cường khả năng tích hợp với hệ thống nguồn phục vụ các sản phẩm Tầng 2, Tầng 3; hoàn thiện các mô đun nền tảng đáp ứng yêu cầu mở rộng; nâng cao khả năng giám sát, dự phòng và ứng cứu sự cố.

3. Triển khai sản phẩm, ứng dụng

Thành phố triển khai 10 sản phẩm ứng dụng phân thành 04 tầng theo mức độ sẵn sàng, điều kiện dữ liệu và cơ chế áp dụng, bảo đảm không triển khai dàn trải và không áp dụng cùng một cơ chế cho mọi nhóm sản phẩm. Mỗi sản phẩm được quản lý theo 04 mốc triển khai gồm chuẩn bị, kiểm thử, bắt đầu vận hành và mở rộng có điều kiện; làm căn cứ xác định trình tự triển khai, theo dõi tiến độ, đánh giá kết quả và xem xét mở rộng. Lộ trình triển khai 10 sản phẩm theo 04 mốc được thể hiện tại Bảng 4.

Bảng 4. Lộ trình triển khai 10 sản phẩm theo 04 mốc

Sản phẩm	Tầng cấp độ	Chuẩn bị	Kiểm thử	Bắt đầu vận hành	Mở rộng có điều kiện
SP1	Tầng 1	2026	2026	2027	2028-2030
SP2	Tầng 1	2026	2026	2027	2028-2030
SP3	Tầng 2	2026-2027	2028	2029	2030
SP4	Tầng 2	2026-2027	2028	2029	2030
SP5	Tầng 3	2026-2027	2028	2029	2030
SP6	Tầng 3	2026-2027	2028	2029	2030
SP7	Tầng 3	2026-2027	2028	2029	2030
SP8	Tầng 4	Đã hoàn thành (trước khi ban hành Đề án)	Đã hoàn thành (trước khi ban hành Đề án)	Đang vận hành (theo cơ chế sandbox)	Theo quy định tại thời điểm xem xét do cơ quan có thẩm quyền quyết định

Sản phẩm	Tầng cấp độ	Chuẩn bị	Kiểm thử	Bắt đầu vận hành	Mở rộng có điều kiện
SP9	Tầng 4	2026-2027	2028	2029	2030
SP10	Tầng 4	2026-2027	2028	2029	2030

Ghi chú: Các mốc đối với SP8 phản ánh trạng thái thực tế tại thời điểm lập Đề án. SP8 tiếp tục thực hiện theo Nghị quyết số 55/2024/NQ-HĐND trong phạm vi, đối tượng, thời gian đã được phê duyệt. Trách nhiệm giám sát theo thẩm quyền cơ chế sandbox đã cấp phép. Đề án chỉ theo dõi trạng thái kết nối kỹ thuật giữa SP8 và DNC-Chain (nếu triển khai).

Điều kiện xác lập 04 mốc triển khai đối với các sản phẩm thuộc Tầng 1, Tầng 2 và Tầng 3 (đối với SP9 và SP10, điều kiện xác lập mốc được thực hiện theo cơ chế riêng gắn với IFC và quyết định của cơ quan có thẩm quyền):

- Mốc chuẩn bị: hoàn thành phân tích và chuẩn hoá tối thiểu 80% dữ liệu nguồn; rà soát pháp lý; xác định đầu mối chủ trì dữ liệu nguồn; ban hành kế hoạch chi tiết cho mốc kiểm thử;

- Mốc kiểm thử: hoàn thành phát triển và tích hợp với DNC-Chain, hệ thống nguồn; đạt yêu cầu kiểm tra kỹ thuật, ATTT và BVDLCN; có dữ liệu vận hành thử tối thiểu một chu kỳ đánh giá;

- Mốc bắt đầu vận hành: được cho phép đưa vào vận hành; đáp ứng điều kiện kỹ thuật, an toàn, pháp lý; có khả năng đo lường chỉ tiêu đầu ra;

- Mốc mở rộng có điều kiện: vận hành ổn định tối thiểu một chu kỳ, đạt chỉ tiêu mốc bắt đầu vận hành; bảo đảm điều kiện mở rộng và cơ quan có thẩm quyền cho phép.

4. Chuẩn hóa dữ liệu, tích hợp hệ thống, bảo đảm an toàn và an ninh

Thành phố tổ chức chuẩn hóa dữ liệu nguồn, bảo đảm chất lượng dữ liệu trong tích hợp, thực hiện đầy đủ các biện pháp bảo đảm ATTT, ANM, BVDLCN và thiết lập cơ chế kiểm tra, đánh giá, kiểm soát tuân thủ trong toàn bộ quá trình triển khai DNC-Chain và các ứng dụng kết nối.

Trong giai đoạn 2026-2027, hoàn thành chuẩn hoá và bảo đảm sẵn sàng dữ liệu nguồn cho các sản phẩm Tầng 1, bám sát Khung kiến trúc dữ liệu quốc gia và Danh mục dữ liệu quan trọng, dữ liệu cốt lõi; thiết lập cơ chế đối soát, xử lý sai lệch giữa hệ thống nguồn, nền tảng tích hợp và DNC-Chain; triển khai đầy đủ các biện pháp ATTT, ANM, BVDLCN, quản lý truy cập, lưu vết, giám sát vận hành và ứng cứu sự cố; tổ chức kiểm tra, đánh giá tuân thủ trước khi đưa hệ thống, ứng dụng vào vận hành.

Trong giai đoạn 2028-2030, mở rộng phạm vi chuẩn hoá đối với dữ liệu phục vụ các sản phẩm Tầng 2, Tầng 3 và các ứng dụng kinh tế dữ liệu; nâng cao năng lực giám sát, phát hiện bất thường, ứng cứu sự cố; duy trì kiểm tra, đánh giá, kiểm soát tuân thủ định kỳ và đột xuất; cập nhật các biện pháp bảo đảm an toàn theo tiến trình hoàn thiện TCVN/QCVN.

5. Nguồn nhân lực, hệ sinh thái và đổi mới sáng tạo

Thành phố phát triển đồng bộ nguồn nhân lực, hệ sinh thái doanh nghiệp, viện nghiên cứu và cơ sở đào tạo; ban hành và triển khai các cơ chế hỗ trợ hệ sinh thái blockchain gắn với chủ trương phát triển công nghệ chiến lược của quốc gia; thúc đẩy hợp tác quốc tế để tăng năng lực triển khai Đề án.

Trong giai đoạn 2026-2027, thực hiện các nhiệm vụ:

- Ban hành Khung năng lực vận hành hệ thống blockchain thành phố làm căn cứ đào tạo, tuyển dụng và bố trí nhân lực;

- Tổ chức đào tạo, bồi dưỡng đội ngũ nhân lực theo vai trò phục vụ vận hành DNC-Chain và các sản phẩm Tầng 1;

- Đưa nội dung blockchain vào chương trình đào tạo của các cơ sở giáo dục đại học, cao đẳng trên địa bàn;

- Ban hành Kế hoạch cụ thể hoá cơ chế thành phố là khách hàng đầu tiên đối với sản phẩm blockchain theo Quyết định số 2815/QĐ-TTg;

- Ban hành Danh mục định hướng đặt hàng nhiệm vụ nghiên cứu, phát triển ứng dụng blockchain cấp thành phố và Kế hoạch phối hợp với Chương trình công nghệ chiến lược quốc gia theo Quyết định số 2815/QĐ-TTg;

- Từng bước hình thành mạng lưới doanh nghiệp, viện nghiên cứu, cơ sở đào tạo tham gia hệ sinh thái.

Trong giai đoạn 2028-2030, mở rộng quy mô đào tạo phục vụ các sản phẩm Tầng 2, Tầng 3 và Tầng 4; triển khai có hiệu quả cơ chế thành phố là khách hàng đầu tiên; tổ chức thực hiện đặt hàng nghiên cứu theo Danh mục đã ban hành, phối hợp chặt chẽ với Chương trình công nghệ chiến lược quốc gia; thúc đẩy hợp tác quốc tế, chuyển giao công nghệ và thu hút chuyên gia blockchain. Đến năm 2030, phấn đấu đạt tối thiểu 1.000 nhân lực blockchain trên địa bàn, 30 doanh nghiệp tham gia hệ sinh thái và 08 nhiệm vụ đặt hàng nghiên cứu cấp thành phố về blockchain.

CHƯƠNG IV: NHIỆM VỤ VÀ GIẢI PHÁP THỰC HIỆN

I. VỀ THỂ CHẾ VÀ KHUNG PHÁP LÝ

1. Rà soát, hệ thống hoá các văn bản pháp lý

Tổ chức rà soát toàn bộ hệ thống văn bản của Trung ương, thành phố và các quy định chuyên ngành có liên quan trực tiếp đến phạm vi triển khai của Đề án, bao quát các nhóm nội dung chủ yếu: Dữ liệu, giao dịch điện tử, lưu trữ, xác minh, chia sẻ dữ liệu, văn bằng, chứng chỉ và hồ sơ y tế; ATTT, ANM và BVDLCN; Cơ chế sandbox; cơ chế gắn với IFC và các mô hình có yếu tố TSMH, tài chính số; Chuyển đổi số; công nghệ chiến lược và sản phẩm công nghệ chiến lược, trong đó có hạ tầng mạng blockchain và các lớp ứng dụng truy xuất nguồn gốc, TSMH; Tiêu chuẩn, quy chuẩn kỹ thuật áp dụng cho công nghệ blockchain, trí tuệ nhân tạo, nền tảng dữ liệu, ATTT và ANM theo hướng dẫn của Bộ Khoa học và Công nghệ, Bộ Công an và các cơ quan liên quan.

Đối với các mô hình thuộc Tầng 4, việc rà soát phải làm rõ giới hạn áp dụng của Đề án và phạm vi điều phối của thành phố. Đây là cơ sở quan trọng để giữ đúng ranh giới giữa nội dung quản lý nhà nước của thành phố với nội dung vận hành theo cơ chế riêng, phân đầu tư và hoạt động thương mại của doanh nghiệp.

Trên cơ sở rà soát, phân loại rõ các nội dung theo nhóm: nội dung đã có đủ căn cứ để triển khai ngay theo quy định hiện hành; nội dung cần được cụ thể hóa bằng quy định, hướng dẫn hoặc quy chế của thành phố; nội dung phải thực hiện theo pháp luật chuyên ngành, cơ chế riêng hoặc theo quyết định của cơ quan có thẩm quyền; nội dung có khả năng được lồng ghép triển khai thông qua Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai ngay. Tránh tình trạng áp dụng vượt thẩm quyền, đồng thời bảo đảm các cơ quan, đơn vị có căn cứ rõ ràng khi tham gia triển khai.

Kết quả rà soát là cơ sở để xây dựng Danh mục văn bản pháp luật cần ban hành, sửa đổi, bổ sung hoặc hướng dẫn thực hiện trong phạm vi Đề án, bao gồm các Quy chế và bộ tiêu chuẩn cụ thể; các văn bản khác phát sinh trong quá trình triển khai; xác định rõ cơ quan chủ trì, cơ quan phối hợp và thời điểm hoàn thành đối với từng văn bản. Việc hoàn thiện cơ sở pháp lý phải bảo đảm đúng thẩm quyền của địa phương, bám sát quy định hiện hành của Trung ương, nhưng đủ cụ thể để xử lý các yêu cầu phát sinh trong quá trình tổ chức thực hiện.

2. Ban hành Quy chế quản trị, vận hành và khai thác DNC-Chain

Ban hành quy chế quản trị, vận hành và khai thác DNC-Chain làm căn cứ quản lý thống nhất đối với hạ tầng blockchain dùng chung của thành phố. Quy chế xác định rõ mô hình quản trị mạng có cấp phép; nguyên tắc tổ chức thành viên mạng; điều kiện tham gia, thay đổi, tạm dừng hoặc chấm dứt tham gia. Quy chế cũng quy định rõ quyền và trách nhiệm của cơ quan quản trị mạng, đơn vị vận hành kỹ thuật, đơn vị chủ trì ứng dụng, cơ quan quản lý dữ liệu nguồn và các chủ thể tích hợp có liên quan trong phạm vi vận hành mạng.

Quy chế quy định cụ thể cơ chế quản lý node, quyền vận hành, quyền xác minh, quyền thay đổi cấu hình, quyền khai thác dữ liệu, quyền truy cập nhật ký và quyền kết nối ứng dụng mới vào DNC-Chain; nguyên tắc phân quyền theo chức năng, nhiệm vụ; cơ chế phê duyệt kết nối; quy trình theo dõi, kiểm tra, giám sát trong toàn bộ vòng đời vận hành. Quy chế quy định đầy đủ cơ chế quản lý định danh kỹ thuật, quản lý khoá mật mã, lưu vết giao dịch, sao lưu, khôi phục, xử lý sự cố và kiểm tra tuân thủ. Việc quản lý, khai thác DNC-Chain phải phân định rõ trách nhiệm, giới hạn quyền hạn, quy trình xử lý và cơ chế kiểm tra, hậu kiểm; đây là điều kiện để DNC-Chain được vận hành như một hạ tầng kỹ thuật dùng chung có kiểm soát, không sử dụng phân tán hoặc vượt phạm vi của Đề án.

Ban hành quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời đối với các ứng dụng kết nối với DNC-Chain, làm rõ trình tự xem xét ứng dụng mới, điều kiện dữ liệu, điều kiện tích hợp, yêu cầu tuân thủ, tiêu chí chuyển giai đoạn theo 04 mốc (chuẩn bị, kiểm thử, bắt đầu vận hành, mở rộng có điều kiện). Bảo đảm mọi ứng dụng được triển khai trên cùng một mặt bằng quản trị thống nhất, có căn cứ giám sát và có cơ sở đánh giá kết quả sau triển khai.

3. Ban hành tiêu chuẩn, yêu cầu kết nối, chia sẻ và kiểm chứng dữ liệu

Xây dựng bộ tiêu chuẩn, yêu cầu kết nối, chia sẻ và kiểm chứng dữ liệu áp dụng cho DNC-Chain bảo đảm phù hợp với Khung kiến trúc Chính phủ số Việt Nam, Khung kiến trúc tổng thể quốc gia số và Khung kiến trúc dữ liệu quốc gia; Khung kiến trúc số của thành phố, bám sát danh mục tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về công nghệ blockchain, nền tảng dữ liệu, ATTT và ANM do Bộ Khoa học và Công nghệ, Bộ Công an ban hành và hướng dẫn áp dụng. Bảo đảm thống nhất giữa khung tiêu chuẩn của thành phố với khung tiêu chuẩn quốc gia, tạo điều kiện để các ứng dụng trên DNC-Chain có thể liên thông, đối soát và tham gia vào các sản phẩm, chương trình chung của quốc gia khi đủ điều kiện.

Bộ tiêu chuẩn áp dụng đối với các hệ thống kết nối DNC-Chain bao quát hai lớp nội dung chính. Về lớp dữ liệu: cấu trúc dữ liệu, dữ liệu đầu vào, siêu dữ liệu, mã tham chiếu, cơ chế ghi nhận bằng chứng xác minh, cơ chế lưu dấu thời gian, chuẩn kiểm chứng, chuẩn ký số và quản lý khoá mật mã. Về lớp kết nối kỹ thuật: định danh kết nối, chuẩn thông điệp, chuẩn giao tiếp dịch vụ, chuẩn tích hợp với nền tảng tích hợp, chia sẻ dữ liệu của thành phố (LGSP), xác minh truy cập, phân quyền khai thác, lưu vết giao dịch và nhật ký, đối soát trạng thái, giám sát vận hành và khả năng mở rộng theo lộ trình. Quy định điều kiện tối thiểu để một hệ thống được phép kết nối với DNC-Chain, bao gồm mức độ sẵn sàng của dữ liệu, khả năng tích hợp, yêu cầu an toàn, an ninh, bảo vệ dữ liệu và khả năng vận hành.

Quá trình triển khai, bộ tiêu chuẩn được định kỳ rà soát, cập nhật phù hợp với sự phát triển của danh mục tiêu chuẩn, quy chuẩn kỹ thuật quốc gia và các hướng dẫn mới của Bộ Khoa học và Công nghệ; kết quả rà soát được công bố thống nhất và áp dụng cho toàn bộ hệ thống kết nối với DNC-Chain. Sở Khoa học và Công nghệ chủ động phối hợp với các đơn vị trực thuộc Bộ Khoa học và Công nghệ, Bộ ngành liên quan trong quá trình xây dựng, rà soát, cập nhật bộ tiêu chuẩn và yêu cầu kỹ thuật áp dụng cho DNC-Chain.

4. Ban hành Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án

Ban hành Quy chế phối hợp liên ngành để bảo đảm quá trình triển khai Đề án được tổ chức thống nhất từ khâu chuẩn bị, thẩm định, tích hợp, vận hành đến giám sát, đánh giá và điều chỉnh. Ở cấp độ toàn Đề án, xác định rõ đầu mối điều phối chung; trách nhiệm của cơ quan chủ trì từng nhóm nội dung; trách nhiệm của cơ quan quản lý dữ liệu nguồn theo lĩnh vực chuyên ngành; trách nhiệm của các tổ chức, doanh nghiệp tham gia cung cấp giải pháp, hạ tầng hoặc dịch vụ hỗ trợ. Phân vai này bổ sung cho quy chế quản trị nội bộ DNC-Chain tại Khoản 2, bao quát toàn bộ các chủ thể liên quan đến Đề án, không giới hạn ở mạng DNC-Chain.

Đối với các nội dung có liên quan đến nhiều ngành, hệ thống hoặc nhiều cấp quản lý, quy định rõ quy trình trao đổi, lấy ý kiến, thẩm định chuyên môn, thẩm định kỹ thuật, kiểm tra an toàn và thống nhất phương án triển khai trước khi đưa vào thực hiện. Làm rõ cơ chế phối hợp giữa cơ quan quản lý nhà nước với đơn vị kỹ thuật để xử lý các vấn đề về chuẩn dữ liệu, kết nối hệ thống, phân quyền truy cập, thay đổi quy trình nghiệp vụ, điều chỉnh phạm vi ứng dụng và xử lý sự cố phát sinh trong quá trình vận hành.

Quy chế bao gồm quy trình xử lý vướng mắc trong quá trình triển khai. Những vấn đề thuộc thẩm quyền của thành phố phải được tổng hợp, phân công rõ đầu mối giải quyết và thời hạn xử lý. Những vấn đề vượt thẩm quyền hoặc có liên quan đến pháp luật chuyên ngành phải được kịp thời tổng hợp, báo cáo và đề xuất cơ quan có thẩm quyền xem xét. Hạn chế tình trạng ách tắc do không rõ đầu mối, không rõ trình tự xử lý hoặc chồng chéo trách nhiệm giữa các cơ quan, đơn vị.

Đối với các mô hình thực hiện theo cơ chế riêng, nhất là các mô hình gắn với IFC hoặc cơ chế sandbox, Quy chế phối hợp phải xác định rõ vai trò điều phối của thành phố, phạm vi hỗ trợ kỹ thuật, phạm vi quản lý nhà nước và cơ chế phối hợp với cơ quan chuyên ngành, cơ quan cấp phép và doanh nghiệp thực hiện. Đây là điều kiện để giữ đúng giới hạn của Đề án, đồng thời vẫn bảo đảm tính liên thông, phối hợp và quản lý rủi ro trong phạm vi cần thiết.

5. Ban hành Quy chế bảo đảm ATTT, ANM và BVDLCN cho DNC-Chain

Ban hành Quy chế bảo đảm ATTT, ANM và BVDLCN áp dụng cho DNC-Chain và các ứng dụng kết nối, cụ thể hoá Luật An toàn thông tin mạng số 86/2015/QH13, Luật An ninh mạng số 24/2018/QH14 và Luật An ninh mạng số 116/2025/QH15 (có hiệu lực thi hành kể từ ngày 01/7/2026, hợp nhất và thay thế hai Luật trên), Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, Nghị định số 356/2025/NĐ-CP của Chính phủ và các quy định chuyên ngành có liên quan. Quy chế bám sát các tiêu chuẩn, quy chuẩn kỹ thuật áp dụng đối với công nghệ blockchain do Bộ Khoa học và Công nghệ và các cơ quan có thẩm quyền ban hành, trong đó có TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ; đồng thời áp dụng kết hợp các tiêu chuẩn quốc tế chuyên ngành chuỗi khối đã được đặc tả tại Phụ lục I. Sở Khoa học và Công nghệ là chủ quản hệ thống thông tin DNC-Chain theo Luật An ninh mạng số 116/2025/QH15, chịu trách nhiệm bảo đảm an toàn hệ thống thông tin theo cấp độ; trách nhiệm cụ thể của đơn vị vận hành kỹ thuật, đơn vị quản lý dữ liệu nguồn và các chủ thể tham gia được phân định tại Quy chế

quản trị, vận hành DNC-Chain quy định tại Khoản 2 Mục này. Việc cập nhật được thực hiện theo lộ trình hoàn thiện khung tiêu chuẩn quốc gia để bảo đảm các yêu cầu an toàn, an ninh của DNC-Chain đồng bộ với mặt bằng chung của quốc gia.

Quy chế quy định rõ nguyên tắc phân loại dữ liệu, nguyên tắc tối thiểu hoá dữ liệu ghi nhận trên DNC-Chain, cơ chế kiểm soát truy cập, phân quyền sử dụng, lưu vết, giám sát và hậu kiểm. Đối với dữ liệu nghiệp vụ, dữ liệu cá nhân và dữ liệu chuyên ngành nhạy cảm, xác định rõ phạm vi xử lý, phạm vi chia sẻ và phương thức kiểm chứng phù hợp, bảo đảm đúng mục đích, đúng thẩm quyền và đúng quy định của pháp luật về BVĐLCN và các quy định chuyên ngành có liên quan.

II. VỀ XÂY DỰNG HẠ TẦNG DNC-CHAIN

1. Tổ chức triển khai hạ tầng DNC-Chain

Thành phố tổ chức triển khai DNC-Chain làm hạ tầng blockchain dùng chung của thành phố, nhằm bảo đảm mặt bằng kỹ thuật thống nhất và khả năng quản lý, giám sát tập trung. Lộ trình triển khai hạ tầng DNC-Chain bám 04 mốc (chuẩn bị, kiểm thử, bắt đầu vận hành, mở rộng có điều kiện), hân kỳ thực hiện được tổ chức theo 02 giai đoạn 2026-2027 và 2028-2030.

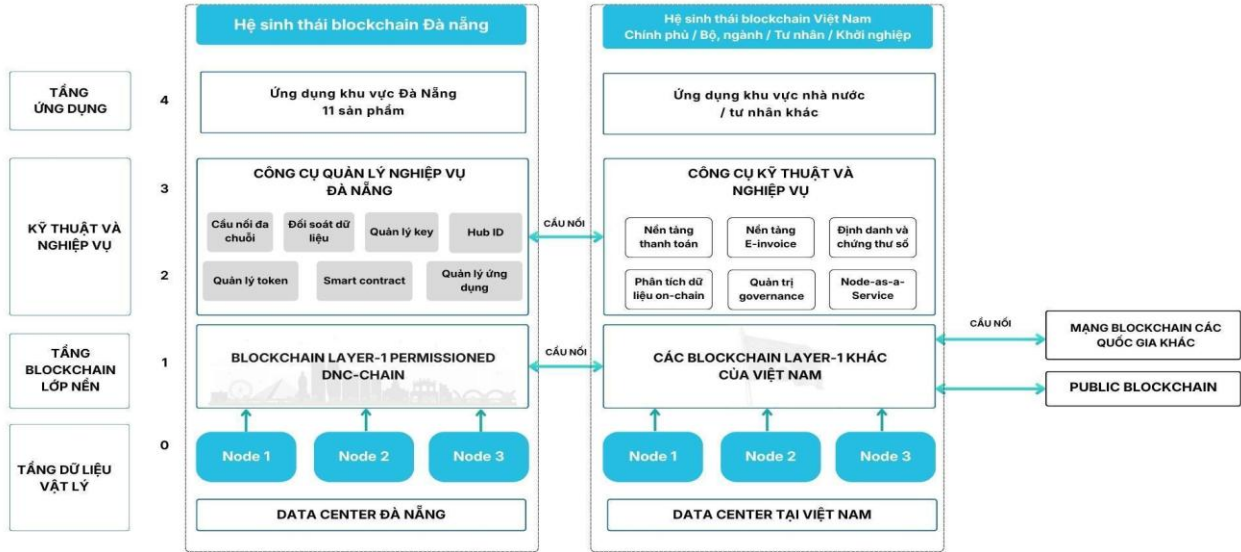
Trong tổ chức triển khai, phân vai rõ giữa cơ quan quản trị mạng, đơn vị vận hành kỹ thuật, cơ quan chủ trì ứng dụng, đơn vị quản lý dữ liệu nguồn và các tổ chức, doanh nghiệp tham gia hỗ trợ kỹ thuật, tích hợp hoặc cung cấp dịch vụ theo Quy chế quản trị, vận hành DNC-Chain. Thành phố chủ động sử dụng, sắp xếp và khai thác hợp lý hạ tầng số hiện có; đồng thời xem xét phương án thuê dịch vụ, hợp tác kỹ thuật hoặc huy động doanh nghiệp tham gia trong những phần việc phù hợp, trên cơ sở bảo đảm vai trò quản lý nhà nước, chủ quyền dữ liệu, khả năng kiểm soát vận hành và yêu cầu an toàn, an ninh của hệ thống.

2. Lựa chọn nền tảng công nghệ Layer-1 của DNC-Chain

Thành phố lựa chọn nền tảng công nghệ lõi của DNC-Chain là chuỗi khối lớp 1 có cấp phép (permissioned Layer-1), tương thích EVM; thuyết minh lựa chọn công nghệ được trình bày tại Bảng 2 Phụ lục I kèm theo Đề án. Đây là lựa chọn phù hợp với các nhóm ứng dụng ưu tiên của DNC-Chain gồm chính quyền số, dịch vụ công, định danh số và quản lý hành chính; bảo đảm khả năng triển khai smart contract, các mô đun nền tảng và nhiều nhóm ứng dụng trên một hạ tầng thống nhất; có hệ sinh thái công cụ phát triển, kiểm toán smart contract và đào tạo nhân lực phong phú; đồng thời bảo đảm khả năng kế thừa các giao thức Lớp nền của kiến trúc đa chuỗi cấp quốc gia.

Thành phố ưu tiên nền tảng blockchain có công nghệ lõi do doanh nghiệp, tổ chức Việt Nam làm chủ. việc áp dụng ưu tiên chỉ thực hiện khi nền tảng đáp ứng đầy đủ các yêu cầu về năng lực kỹ thuật, khả năng quản trị mạng có cấp phép, hiệu năng, ATTT, ANM, khả năng tích hợp với kiến trúc số của thành phố và khả năng mở rộng theo lộ trình. Trường hợp điều kiện kỹ thuật và quản trị chưa được bảo đảm, không áp dụng ưu tiên. Nền tảng được lựa chọn phải bảo đảm trung lập công nghệ, không phụ thuộc một nhà cung cấp duy nhất và khả năng tương thích với các chuẩn kết nối phù hợp cho yêu cầu tích hợp và liên thông, phù hợp với nguyên tắc đã nêu.

3. Tổ chức mô hình kiến trúc mạng, node



Hình 3: Mô hình kiến trúc Mạng DNC-Chain kết nối mạng blockchain khác

DNC-Chain được tổ chức theo mô hình kiến trúc mạng có cấp phép, trong đó việc tham gia mạng, vận hành node, xác minh giao dịch và thay đổi cấu hình đều phải được kiểm soát theo quy chế quản trị thống nhất của thành phố. Kiến trúc mạng phải bảo đảm vừa đáp ứng yêu cầu vận hành ổn định, vừa bảo đảm khả năng kiểm soát chặt chẽ đối với thành viên tham gia, quyền truy cập và trách nhiệm của từng chủ thể.

Kiến trúc mạng được tổ chức theo mô hình nhiều node, phân tán trên các hạ tầng độc lập và phân vai theo chức năng vận hành, gồm node quản trị mạng (governance node), node xác minh (validator node) và node hỗ trợ kỹ thuật (service node). Trên cơ sở yêu cầu bố trí hạ tầng phân tán tại tối thiểu 03 địa điểm độc lập, cấu hình tối thiểu của DNC-Chain được tổ chức theo từng giai đoạn như quy định tại Bảng 5.

Bảng 5. Cấu hình node tối thiểu theo giai đoạn

Giai đoạn	Thành phần	Số lượng	Địa điểm bố trí	Vai trò
2026-2027	Node quản trị mạng	01	01 cơ sở nhà nước độc lập	Điều phối cấu hình mạng, quản lý danh sách node được cấp phép, phê duyệt thay đổi thành phần mạng, kiểm soát trạng thái vận hành chung
2026-2027	Validator node	01	Hạ tầng nhà nước phù hợp theo phương án được phê duyệt	Xác minh giao dịch, tham gia đồng thuận, tạo block, duy trì trạng thái sổ cái

Giai đoạn	Thành phần	Số lượng	Địa điểm bố trí	Vai trò
2026-2027	Node hỗ trợ kỹ thuật (service node)	02	Trung tâm dữ liệu doanh nghiệp trên địa bàn thành phố đáp ứng điều kiện kỹ thuật, an toàn, an ninh	Hỗ trợ giám sát, tích hợp, sao lưu, phục hồi, kết nối và các chức năng kỹ thuật phục vụ vận hành mạng
Đến 2030	Node quản trị mạng	02	02 cơ sở nhà nước độc lập	Duy trì cơ chế quản trị mạng có cấp phép, kiểm soát cấu hình, quản lý thành viên mạng
Đến 2030	Validator node	02	Tối thiểu 01 vị trí hạ tầng nhà nước; phần còn lại tại hạ tầng đáp ứng điều kiện kỹ thuật theo phương án được phê duyệt	Xác minh giao dịch, mở rộng khả năng vận hành, tăng dự phòng và nâng cao tính sẵn sàng
Đến 2030	Node hỗ trợ kỹ thuật (service node)	02	Hạ tầng doanh nghiệp hoặc hạ tầng phù hợp theo phương án được phê duyệt	Hỗ trợ giám sát, tích hợp, sao lưu, phục hồi, kết nối và bảo đảm vận hành kỹ thuật toàn mạng

Ghi chú: Giai đoạn 2026-2027 vận hành thử với cấu hình tối thiểu nhằm kiểm chứng quy trình quản trị, tích hợp, an toàn vận hành và năng lực phối hợp giữa các bên tham gia; cơ chế đồng thuận phân tán đầy đủ theo nguyên lý Byzantine Fault Tolerance (tối thiểu 04 validator node trên các địa điểm độc lập) được áp dụng từ giai đoạn 2028-2030 trở đi theo phương án được phê duyệt.

Trong các giai đoạn tiếp theo, căn cứ vào số lượng ứng dụng tiếp nhận, nhu cầu xử lý giao dịch, điều kiện hạ tầng và yêu cầu bảo đảm tính sẵn sàng, thành phố xem xét mở rộng thêm validator node và các node hỗ trợ kỹ thuật khi cần thiết. Việc mở rộng phải phù hợp với lộ trình triển khai, không làm thay đổi nguyên tắc quản trị mạng, không làm phát sinh kiến trúc phân tán thiếu kiểm soát và không ảnh hưởng đến tính ổn định của DNC-Chain trong quá trình vận hành. Đối với các node do doanh nghiệp vận hành, cơ quan đầu mối quản lý hạ tầng phải duy trì phương án dự phòng kỹ thuật để bảo đảm khả năng thay thế node khi phát sinh sự cố hoặc gián đoạn vận hành; phương án này phải được cập nhật, kiểm tra định kỳ và gắn với kế hoạch sao lưu, phục hồi của toàn hệ thống.

Các chức năng của DNC-Chain và quy trình quản lý vòng đời node được xác định tại Phụ lục I kèm theo Đề án.

4. Xây dựng các mô đun nền tảng dùng chung của DNC-Chain

Các mô đun nền tảng dùng chung của DNC-Chain được xây dựng theo nguyên tắc tái sử dụng, cho phép nhiều sản phẩm cùng khai thác trên một hạ tầng thống nhất thay vì phát triển riêng lẻ cho từng ứng dụng. 07 mô đun gồm: Cầu nối Đa chuỗi; Tích hợp, tạo bằng chứng xác minh và đối soát hồ sơ điện tử; Quản lý khoá và phân quyền; Quản lý giao dịch và token; Quản lý smart contract; Quản lý ứng dụng và marketplace; Hub làm sạch dữ liệu. Các mô đun có thể được nâng cấp, thay thế hoặc mở rộng theo từng giai đoạn triển khai mà không làm thay đổi kiến trúc lõi. Thuyết minh kỹ thuật chi tiết của từng mô đun được trình bày tại Phụ lục I kèm theo Đề án.

a) Mô đun 1: Cầu nối Đa chuỗi

Mục tiêu và phạm vi: Xây dựng mô đun liên thông phục vụ trao đổi thông điệp, bằng chứng xác minh và trạng thái nghiệp vụ giữa DNC-Chain với nền tảng quốc gia, các blockchain, nền tảng ngoài phạm vi hệ thống của thành phố khi có nhu cầu thực tiễn và được cấp có thẩm quyền cho phép. Mô đun này không phục vụ chuyển giao tài sản xuyên chuỗi và không sao chép dữ liệu nghiệp vụ gốc.

Nội dung xây dựng: Xây dựng thành phần phát hành, tiếp nhận, xác minh và chuyển tiếp thông điệp liên chuỗi; cơ chế quản lý danh mục chuỗi và smart contract được phép kết nối; cơ chế hàng đợi, thử lại, giám sát, lưu vết, cảnh báo và ngắt kết nối khi phát hiện bất thường; cơ chế quản trị thay đổi đối với danh sách kết nối và các tham số vận hành.

Kết quả đầu ra: Hình thành mô đun liên thông có kiểm soát giữa DNC-Chain với các nền tảng được phép kết nối, phục vụ xác minh, đối soát, chia sẻ trạng thái và hỗ trợ liên thông kỹ thuật theo phạm vi được phê duyệt.

Giai đoạn ưu tiên triển khai: Giai đoạn 2026-2027 xây dựng chức năng liên thông ở mức phục vụ nhu cầu ưu tiên. Giai đoạn 2028-2030 hoàn thiện và mở rộng theo danh mục kết nối được phê duyệt.

b) Mô đun 2: Tích hợp, tạo bằng chứng xác minh và đối soát hồ sơ điện tử

Mục tiêu và phạm vi: Xây dựng mô đun trung gian chuyên biệt để tiếp nhận dữ liệu từ hệ thống nguồn và nền tảng tích hợp, chia sẻ dữ liệu của thành phố, tạo bằng chứng xác minh trên DNC-Chain và hỗ trợ đối soát, kiểm chứng hồ sơ điện tử. Mô đun này không thay thế sản phẩm ứng dụng; đây là cầu phần kỹ thuật dùng chung phục vụ nhiều ứng dụng có nhu cầu xác minh và đối soát.

Nội dung xây dựng: Xây dựng công cụ tạo giá trị băm, gom giao dịch, đóng dấu thời gian, ghi nhận bằng chứng lên DNC-Chain, trả biên lai xác minh, hỗ trợ kiểm chứng và đối soát hồ sơ; xây dựng giao diện tra cứu, xác minh bằng chứng; xây dựng thư viện tích hợp để các hệ thống nghiệp vụ kết nối và khai thác thống nhất.

Kết quả đầu ra: Hình thành mô đun dùng chung phục vụ tạo bằng chứng xác minh, kiểm chứng và đối soát đối với hồ sơ điện tử, giao dịch và sự kiện nghiệp vụ; làm nền tảng kỹ thuật cho các ứng dụng có nhu cầu bảo đảm toàn vẹn, truy vết và hậu kiểm.

Giai đoạn ưu tiên triển khai: Giai đoạn 2026-2027 ưu tiên xây dựng để phục vụ các ứng dụng trọng tâm thuộc Tầng 1. Giai đoạn 2028-2030 mở rộng phạm vi áp dụng cho các ứng dụng có dữ liệu phức tạp hơn và yêu cầu đối soát cao hơn.

c) Mô đun 3: Quản lý khoá và phân quyền

Mục tiêu và phạm vi: Xây dựng mô đun quản lý vòng đời khoá mật mã, định danh kỹ thuật và phân quyền truy cập cho các tổ chức, cá nhân, hệ thống và ứng dụng tham gia DNC-Chain. Đây là mô đun nền tảng bảo đảm an toàn vận hành và kiểm soát quyền tham gia trong toàn bộ hệ sinh thái DNC-Chain.

Nội dung xây dựng: Xây dựng hạ tầng quản lý khoá; cơ chế tạo lập, phân phối, luân phiên, thu hồi, sao lưu và phục hồi khoá; cơ chế phân quyền theo vai trò đối với mạng, tổ chức, ứng dụng và dịch vụ; cơ chế xác minh chủ thể tham gia; cơ chế ghi nhận, lưu vết và giám sát mọi thay đổi về khoá và phân quyền.

Kết quả đầu ra: Hình thành mô đun dùng chung phục vụ quản lý khoá, xác minh chủ thể và kiểm soát phân quyền truy cập đối với toàn bộ hạ tầng, ứng dụng và dịch vụ trên DNC-Chain; bảo đảm rõ quyền, rõ trách nhiệm và có căn cứ phục vụ giám sát, kiểm tra, kiểm toán.

Giai đoạn ưu tiên triển khai: Giai đoạn 2026-2027 triển khai đồng bộ với hạ tầng DNC-Chain và các mô đun nền tảng dùng chung. Giai đoạn 2028-2030 hoàn thiện, mở rộng và nâng cao theo nhu cầu phát triển ứng dụng và mở rộng kết nối.

d) Mô đun 4: Quản lý giao dịch và Token

Mục tiêu và phạm vi: Xây dựng mô đun quản lý trạng thái giao dịch và các token nội bộ, bao gồm cả token chứng nhận, điểm thưởng và token ghi nhận nghiệp vụ không có chức năng thanh toán phục vụ các ứng dụng trong hệ sinh thái DNC-Chain. Mô đun này chỉ phục vụ các chức năng nghiệp vụ, quản trị, xác minh, chứng nhận, điểm thưởng và các trường hợp được phép trong phạm vi Đề án; không tổ chức thị trường giao dịch TSMH trên hạ tầng dùng chung; mọi mô hình giao dịch TSMH chỉ thực hiện theo pháp luật chuyên ngành và cơ chế riêng tại Tầng 4.

Nội dung xây dựng: Xây dựng công cụ phát hành, quản lý và kiểm soát vòng đời token nội bộ; công cụ quản lý trạng thái giao dịch; sổ theo dõi số dư, lịch sử giao dịch và truy vết giao dịch; cơ chế kiểm soát tuân thủ, giới hạn sử dụng, giới hạn đối tượng nắm giữ và giới hạn chuyển giao theo từng loại token nội bộ.

Kết quả đầu ra: Hình thành mô đun dùng chung phục vụ quản lý giao dịch, quản lý trạng thái token và lưu vết giao dịch đối với các ứng dụng thuộc phạm vi Đề án; tạo cơ sở cho đối soát, kiểm tra, kiểm toán và cung cấp bằng chứng phục vụ giải quyết tranh chấp theo thẩm quyền khi cần thiết.

Giai đoạn ưu tiên triển khai: Giai đoạn 2026-2027 ưu tiên xây dựng các chức năng phục vụ ứng dụng nền tảng và các sản phẩm triển khai sớm. Giai đoạn 2028-2030 mở rộng đối với các ứng dụng của Tầng 3 và phần hỗ trợ kỹ thuật cho Tầng 4 theo phạm vi được phép.

đ) Mô đun 5: Quản lý smart contract

Mục tiêu và phạm vi: Xây dựng mô đun quản lý toàn bộ vòng đời smart contract trên DNC-Chain, từ phát triển, kiểm thử, kiểm toán, phê duyệt, triển khai đến nâng cấp. Đây là mô đun bảo đảm các smart contract được quản lý thống nhất, an toàn và có thể kiểm soát trong toàn bộ hệ sinh thái DNC-Chain.

Nội dung xây dựng: Xây dựng thư viện smart contract chuẩn; quy trình phát triển an toàn; cơ chế kiểm thử, kiểm toán và phê duyệt trước khi triển khai; sổ đăng ký hợp đồng trên chuỗi; cơ chế quản lý phiên bản, thay đổi và nâng cấp hợp đồng; cơ chế ghi nhận ký đầy đủ đối với toàn bộ vòng đời hợp đồng.

Kết quả đầu ra: Hình thành mô đun dùng chung phục vụ quản lý tập trung các smart contract trên DNC-Chain; bảo đảm các hợp đồng được phát triển, kiểm thử, triển khai và vận hành theo quy trình chuẩn hoá, có kiểm soát và có căn cứ phục vụ giám sát, kiểm tra, kiểm toán.

Giai đoạn ưu tiên triển khai: Giai đoạn 2026-2027 ưu tiên xây dựng thư viện và quy trình phục vụ các ứng dụng đầu tiên. Giai đoạn 2028-2030 hoàn thiện, mở rộng theo nhu cầu phát triển ứng dụng và dịch vụ trên DNC-Chain.

e) Mô đun 6: Quản lý ứng dụng và marketplace

Mục tiêu và phạm vi: Xây dựng mô đun quản lý vòng đời ứng dụng trong hệ sinh thái DNC-Chain và hỗ trợ tra cứu, tích hợp, tái sử dụng các giải pháp đã được cấp phép. Mô đun này phục vụ quản lý đăng ký ứng dụng, kiểm soát quyền truy cập, giám sát vận hành và từng bước hình thành marketplace.

Nội dung xây dựng: Xây dựng sổ đăng ký ứng dụng; công tích hợp ứng dụng; bộ công cụ hỗ trợ phát triển và kết nối; môi trường thử nghiệm; công cụ giám sát vận hành ứng dụng; công tra cứu và tái sử dụng ứng dụng; cơ chế cấp phép, thu hồi, theo dõi trạng thái hoạt động và quản lý hạn mức sử dụng của từng ứng dụng.

Kết quả đầu ra: Hình thành mô đun dùng chung phục vụ quản lý tập trung toàn bộ ứng dụng trên DNC-Chain; hỗ trợ mở rộng hệ sinh thái ứng dụng theo cơ chế có kiểm soát; tạo điều kiện để các cơ quan, đơn vị và doanh nghiệp tra cứu, tích hợp và tái sử dụng các giải pháp phù hợp.

Giai đoạn ưu tiên triển khai: Giai đoạn 2026-2027 ưu tiên đăng ký, tích hợp và giám sát các ứng dụng trọng tâm. Giai đoạn 2028-2030 mở rộng kho ứng dụng, cơ chế tái sử dụng và hỗ trợ tích hợp cho các sản phẩm, dịch vụ mở rộng.

g) Mô đun 7: Hub làm sạch dữ liệu

Mục tiêu và phạm vi: Xây dựng mô đun hỗ trợ làm sạch, chuẩn hoá và tách định danh dữ liệu, phục vụ xác minh chủ thể giao dịch trên DNC-Chain mà không ghi thông tin nhận dạng cá nhân lên chuỗi. Mô đun này là cấu phần kỹ thuật bảo đảm vừa hỗ trợ xác minh, vừa tuân thủ yêu cầu BVDLCN trong toàn bộ hệ sinh thái DNC-Chain.

Nội dung xây dựng: Xây dựng cơ chế cấp và quản lý mã định danh kỹ thuật vô danh; cơ chế liên kết với hệ thống nguồn đã thực hiện xác minh ban đầu; cơ chế cấp, kiểm tra và thu hồi chứng thực xác minh số; cơ chế ghi nhận ký truy vấn, sử dụng và tra

cứu ngược theo yêu cầu pháp lý hợp lệ; cơ chế hỗ trợ đánh giá tác động xử lý dữ liệu và kiểm soát tuân thủ đối với các ứng dụng có xử lý dữ liệu cá nhân.

Kết quả đầu ra: Hình thành mô đun dùng chung phục vụ làm sạch dữ liệu, tách định danh và hỗ trợ xác minh chủ thể trên DNC-Chain; bảo đảm dữ liệu cá nhân không ghi trực tiếp lên sổ cái blockchain; tạo cơ sở cho các ứng dụng có xử lý dữ liệu cá nhân vận hành đúng phạm vi, đúng mục đích và có thể kiểm soát.

Giai đoạn ưu tiên triển khai: Giai đoạn 2026-2027 ưu tiên phục vụ các ứng dụng có dữ liệu cá nhân trong Tầng 1. Giai đoạn 2028-2030 hoàn thiện và mở rộng cho các ứng dụng có yêu cầu xác minh, liên thông và bảo vệ dữ liệu cao hơn.

5. Kết nối DNC-Chain với nền tảng tích hợp và các hệ thống nguồn

Việc kết nối DNC-Chain với các hệ thống thông tin, cơ sở dữ liệu và ứng dụng thành phần của thành phố được tổ chức theo kiến trúc thống nhất bốn lớp: hệ thống nguồn tiếp tục quản lý dữ liệu nghiệp vụ gốc; nền tảng tích hợp, chia sẻ dữ liệu của thành phố (LGSP) giữ vai trò đầu mối điều phối kết nối; lớp trung gian chuyên biệt thực hiện chức năng tích hợp kỹ thuật khi cần thiết; DNC-Chain thực hiện vai trò ghi nhận bằng chứng xác minh, lưu vết và hỗ trợ kiểm chứng độc lập.

Không tổ chức kết nối trực tiếp từ các hệ thống nguồn lên DNC-Chain ngoài cơ chế tích hợp đã được phê duyệt. Mỗi kết nối phải được khảo sát, thiết kế, kiểm thử, đối soát và nghiệm thu trước khi đưa vào vận hành chính thức. Việc kết nối phải xác định rõ dữ liệu nào tiếp tục nằm tại hệ thống nguồn, dữ liệu nào được chuyển qua lớp tích hợp, dữ liệu nào được ghi nhận trên DNC-Chain dưới dạng bằng chứng xác minh, dữ liệu tham chiếu hoặc thông tin phục vụ truy vết, hậu kiểm.

Kiến trúc tích hợp kỹ thuật, các cấu phần, quy trình ghi bằng chứng, quy trình xác minh và truy xuất được thuyết minh chi tiết tại Phần B Phụ lục I kèm theo Đề án.

a) Phạm vi và thứ tự ưu tiên kết nối

Giai đoạn đầu, ưu tiên kết nối các hệ thống phục vụ trực tiếp cho các sản phẩm trọng tâm của Đề án, đặc biệt là các sản phẩm có nhu cầu rõ về toàn vẹn hồ sơ điện tử, xác minh văn bằng, chứng chỉ. Trên cơ sở kết quả triển khai thực tế, thành phố từng bước mở rộng kết nối sang các nhóm sản phẩm khác khi đáp ứng đủ điều kiện về dữ liệu, tích hợp, tổ chức thực hiện và an toàn, an ninh.

Việc mở rộng được thực hiện theo lộ trình gắn với mức độ sẵn sàng của dữ liệu nguồn, khả năng tích hợp của hệ thống và nhu cầu xác minh, truy vết, đối soát trong thực tế; không mở rộng đồng loạt, tránh triển khai kết nối vượt khả năng tổ chức thực hiện của cơ quan chủ trì dữ liệu.

b) Nguyên tắc triển khai và mở rộng tích hợp

Việc triển khai tích hợp giữa DNC-Chain với LGSP và các hệ thống nguồn được thực hiện theo các nguyên tắc sau:

- Dữ liệu nghiệp vụ gốc tiếp tục được quản lý tại hệ thống nguồn; không chuyển dữ liệu nghiệp vụ gốc lên DNC-Chain;

- Trên DNC-Chain chỉ ghi nhận bằng chứng mật mã, dữ liệu tham chiếu và thông tin mô tả tối thiểu cần thiết cho kiểm chứng, đối soát và truy vết;

- Mọi kết nối ứng dụng với DNC-Chain phải đi qua lớp tích hợp chuẩn hoá; không tích hợp trực tiếp từ hệ thống nghiệp vụ vào DNC-Chain ngoài cơ chế kiểm soát chung;

- Toàn bộ giao dịch và thông điệp tích hợp phải được ghi nhận ký, giám sát và kiểm soát truy cập theo quy định.

Trường hợp dữ liệu nguồn chưa được chuẩn hoá, chưa bảo đảm chất lượng hoặc hệ thống nguồn chưa đáp ứng yêu cầu kết nối, thành phố ưu tiên chuẩn hóa dữ liệu, nâng cấp hệ thống nguồn, chuẩn hoá giao diện tích hợp và hoàn thiện quy trình quản lý trước khi đưa vào khai thác trên DNC-Chain. Cách tiếp cận này bảo đảm việc mở rộng tích hợp đồng bộ với mức độ sẵn sàng của hệ thống, không để xảy ra tình trạng hạ tầng blockchain được triển khai trước nhưng không khai thác hiệu quả do dữ liệu và đầu nối chưa sẵn sàng.

Bảng 6. Các tiêu chí chính để xem xét mở rộng tích hợp

Tiêu chí	Nội dung xem xét
Nhu cầu nghiệp vụ	Mức độ cần thiết của xác minh, truy vết hoặc đối soát dữ liệu
Mức độ sẵn sàng dữ liệu	Dữ liệu nguồn đã được chuẩn hoá, quản lý ổn định và có khả năng đối soát
Khả năng tích hợp	Hệ thống nguồn có khả năng tích hợp với LGSP và lớp kết nối chuẩn hoá
ATTT	Đáp ứng yêu cầu bảo mật, quản lý truy cập và kiểm soát khai thác
Hiệu quả khai thác	Có giá trị sử dụng rõ ràng trong quản lý nhà nước, dịch vụ công hoặc cung cấp dịch vụ

c) Kết nối với Nền tảng chuỗi khối quốc gia và liên thông với các nền tảng chuỗi khối khác

Việc kết nối, liên thông của DNC-Chain với các nền tảng chuỗi khối thực hiện theo nguyên tắc quy định tại Khoản 2 Mục II Chương III, gồm kết nối mặc định với Nền tảng chuỗi khối quốc gia và liên thông có điều kiện với các nền tảng chuỗi khối khác qua Cầu nối Đa chuỗi. Việc mở rộng tích hợp được thực hiện theo cơ chế kiểm soát chặt chẽ, trên cơ sở danh mục điểm tin cậy (allowlist) do cơ quan chủ trì cấp phép, tiêu chuẩn kỹ thuật tương thích, cơ chế xác minh bằng chứng phù hợp và các biện pháp giám sát kỹ thuật, ATTT theo quy định. Việc kết nối và liên thông không được hiểu là hợp nhất sổ cái, dùng chung một chuỗi hoặc phụ thuộc mặc định vào một hạ tầng blockchain bên ngoài duy nhất.

Trong mọi trường hợp, nguyên tắc tổ chức kết nối của DNC-Chain phải được giữ thống nhất: hệ thống nguồn tiếp tục quản lý dữ liệu nghiệp vụ; LGSP giữ vai trò đầu mối điều phối tích hợp; lớp trung gian chuyên biệt thực hiện chức năng tích hợp kỹ thuật;

DNC-Chain ghi nhận bằng chứng và lưu vết kỹ thuật; các ứng dụng khai thác kết quả xác minh và kiểm chứng theo đúng phạm vi được cấp quyền. Cách tổ chức này giúp DNC-Chain phát huy vai trò là hạ tầng blockchain dùng chung của thành phố, đồng thời bảo đảm tính mở có kiểm soát đối với nhu cầu liên thông trong tương lai.

6. Giám sát, duy trì hoạt động ổn định, dự phòng và ứng cứu sự cố

Thành phố thiết lập cơ chế giám sát toàn diện đối với DNC-Chain nhằm theo dõi trạng thái hoạt động, năng lực xử lý, tính sẵn sàng, mức độ ổn định, nhật ký giao dịch, nhật ký truy cập và các dấu hiệu bất thường trong quá trình vận hành. Cơ chế giám sát phải bảo đảm phát hiện sớm các vấn đề về hiệu năng, an toàn, an ninh, sai lệch trạng thái hoặc rủi ro kỹ thuật để có biện pháp xử lý kịp thời.

Tổ chức các giải pháp duy trì hoạt động ổn định của hạ tầng như bảo trì định kỳ, cập nhật phiên bản, kiểm tra cấu hình, kiểm thử an toàn, sao lưu dữ liệu, dự phòng hệ thống và xây dựng phương án khôi phục sau sự cố. Hệ thống phải có khả năng tiếp tục hoạt động hoặc phục hồi trong thời gian phù hợp khi xảy ra sự cố kỹ thuật, lỗi cấu hình, mất kết nối, mất dữ liệu hoặc các tình huống rủi ro khác ảnh hưởng đến tính liên tục của dịch vụ.

Đồng thời xây dựng cơ chế ứng cứu sự cố đối với DNC-Chain và các kết nối liên quan, trong đó xác định rõ đầu mối tiếp nhận thông tin, quy trình phát hiện, cảnh báo, cô lập, xử lý, khôi phục và báo cáo sau sự cố. Việc ứng cứu sự cố phải được thực hiện theo cơ chế phối hợp chặt chẽ giữa đơn vị vận hành hạ tầng, cơ quan điều phối Đề án, cơ quan chuyên trách về ATTT, ANM và các cơ quan, đơn vị có liên quan. Đồng thời, tổ chức diễn tập, đánh giá và cập nhật phương án ứng cứu theo định kỳ để bảo đảm hệ thống luôn sẵn sàng trước các tình huống phát sinh.

III. VỀ TRIỂN KHAI 10 SẢN PHẨM THEO 04 TẦNG CẤP ĐỘ

Đề án xác định triển khai **10 sản phẩm** (SP1 đến SP10), tổ chức theo 04 tầng và lộ trình đã xác định. Phân công cơ quan chủ trì được thực hiện thống nhất theo hai vai trò: **cơ quan chủ trì sản phẩm** và **cơ quan chủ trì dữ liệu nguồn** trong trường hợp hai chủ thể này không trùng nhau. Cơ quan chủ trì sản phẩm chịu trách nhiệm tổng thể về phạm vi, mục tiêu, lộ trình, kết quả, chỉ tiêu đánh giá và cơ chế phối hợp triển khai. Cơ quan chủ trì dữ liệu nguồn chịu trách nhiệm bảo đảm tính đầy đủ, chính xác, cập nhật và hợp pháp của dữ liệu nghiệp vụ được tích hợp với DNC-Chain.

Thuyết minh kỹ thuật của 10 sản phẩm bao gồm kiến trúc, sơ đồ luồng vận hành và yêu cầu tích hợp được trình bày tại Phụ lục I kèm theo Đề án.

1. Tầng 1 (SP1, SP2)

Tầng 1 gồm 02 sản phẩm có mức độ sẵn sàng tương đối cao, có bài toán thực tiễn rõ, có điều kiện dữ liệu và tích hợp thuận lợi hơn các nhóm còn lại, có đầu mối chủ trì xác định và có khả năng tạo kết quả sử dụng thực tế trong giai đoạn đầu triển khai. Đây là nhóm được ưu tiên tổ chức thực hiện trước trong giai đoạn 2026-2027 để kiểm chứng mô hình lớp tin cậy số trên hạ tầng DNC-Chain.

Bảng 7. Phân công cơ quan chủ trì và phối hợp triển khai các sản phẩm thuộc Tầng 1

SP	Cơ quan chủ trì SP	Cơ quan chủ trì dữ liệu nguồn	Cơ quan phối hợp
SP1	Sở Khoa học và Công nghệ	Các sở, ban, ngành, đơn vị có hệ thống nghiệp vụ và hồ sơ điện tử thuộc phạm vi triển khai	Các đơn vị vận hành hệ thống nghiệp vụ
SP2	Sở Giáo dục và Đào tạo	Các cơ sở giáo dục đại học, cao đẳng, các trường và cơ sở giáo dục nghề nghiệp	Sở Khoa học và Công nghệ

a) SP1. Hệ thống bảo đảm toàn vẹn hồ sơ điện tử trên blockchain

Mục tiêu triển khai: Triển khai SP1 để bảo đảm tính toàn vẹn của hồ sơ điện tử trong quá trình tiếp nhận, xử lý, luân chuyển, chia sẻ và khai thác giữa các cơ quan, đơn vị. Sản phẩm này hỗ trợ xác minh trạng thái hồ sơ, kiểm chứng dữ liệu khi cần thiết và tăng khả năng truy vết, hậu kiểm trong môi trường điện tử. Đây là sản phẩm ưu tiên triển khai sớm vì bám sát yêu cầu quản lý nhà nước, có phạm vi áp dụng rõ và phù hợp với vai trò lớp tin cậy số của DNC-Chain.

Phạm vi và đối tượng áp dụng: Giai đoạn đầu, SP1 áp dụng đối với một số nhóm hồ sơ điện tử có tần suất xử lý lớn, quy trình tương đối ổn định và có nhu cầu kiểm chứng rõ. Đối tượng áp dụng gồm các cơ quan, đơn vị có hệ thống nghiệp vụ tham gia xử lý hồ sơ điện tử; các đơn vị vận hành hệ thống; và các cơ quan, tổ chức có nhu cầu tra cứu, đối soát hoặc xác minh hồ sơ theo quy định. Phạm vi triển khai được xác định theo từng nhóm hồ sơ cụ thể, không thực hiện dàn trải ngay từ đầu.

Mô hình triển khai và thành phần chính: Hệ thống nguồn tiếp tục quản lý hồ sơ điện tử gốc theo chức năng, thẩm quyền của từng cơ quan, đơn vị, phù hợp với quy định của Luật Giao dịch điện tử số 20/2023/QH15 và Luật Dữ liệu số 60/2024/QH15. Nền tảng tích hợp và chia sẻ dữ liệu của thành phố thực hiện kết nối, điều phối giao tiếp dữ liệu theo quy định về kết nối, chia sẻ dữ liệu bắt buộc tại Nghị định số 278/2025/NĐ-CP của Chính phủ và Khung kiến trúc dữ liệu quốc gia tại Quyết định số 2439/QĐ-TTg. SP1 tiếp nhận thông tin cần xác minh, xử lý theo chuẩn thống nhất và ghi nhận bằng chứng xác minh lên DNC-Chain. DNC-Chain chỉ thực hiện vai trò lớp tin cậy số, không thay thế hệ thống nguồn và không lưu trữ hồ sơ điện tử đầy đủ.

Quy trình vận hành chính: Khi hồ sơ điện tử được tạo lập hoặc thay đổi trạng thái tại hệ thống nguồn, thông tin cần xác minh được gửi qua lớp tích hợp. SP1 tiếp nhận, chuẩn hoá dữ liệu tham chiếu và ghi nhận bằng chứng xác minh lên DNC-Chain. Khi có yêu cầu kiểm tra, hệ thống thực hiện đối chiếu giữa dữ liệu hiện tại và bằng chứng đã được ghi nhận để xác định tính toàn vẹn và trạng thái xử lý của hồ sơ. Kết quả xác minh được sử dụng phục vụ tra cứu, giám sát, kiểm tra và hậu kiểm.

Điều kiện triển khai: SP1 chỉ triển khai đối với nhóm hồ sơ có cấu trúc dữ liệu rõ, có mã hồ sơ, có nhật ký trạng thái và có đầu mối quản lý cụ thể. Cơ quan chủ trì sản phẩm, cơ quan chủ trì dữ liệu nguồn và đầu mối phối hợp kỹ thuật phải được xác định rõ.

Hệ thống nguồn phải có khả năng kết nối với nền tảng tích hợp của thành phố theo yêu cầu tại Nghị định số 278/2025/NĐ-CP. Quy trình nghiệp vụ phải đủ rõ để xác định điểm cần xác minh, đối soát và truy vết. Các yêu cầu về ATTT, ANM và bảo vệ dữ liệu phải được rà soát trước khi vận hành.

Nhiệm vụ chủ yếu: Rà soát, lựa chọn nhóm hồ sơ điện tử phù hợp để triển khai. Chuẩn hoá mã hồ sơ, siêu dữ liệu và trạng thái xử lý theo Khung kiến trúc dữ liệu quốc gia và Khung kiến trúc Chính phủ số Việt Nam. Hoàn thiện cơ chế tích hợp giữa hệ thống nguồn, nền tảng tích hợp và SP1. Tổ chức thử nghiệm theo quy trình thực tế. Đánh giá khả năng xác minh, kiểm chứng và đối soát. Hoàn thiện cơ chế khai thác, vận hành và giám sát. Chuẩn bị điều kiện để mở rộng sang các nhóm hồ sơ khác khi đáp ứng yêu cầu.

Kết quả cần đạt: Hình thành được sản phẩm hỗ trợ bảo đảm toàn vẹn hồ sơ điện tử, xác minh trạng thái xử lý và kiểm chứng độc lập giữa các cơ quan, đơn vị trong môi trường số. Tăng khả năng truy vết, đối soát và hậu kiểm đối với các hồ sơ điện tử có nhiều chủ thể tham gia xử lý. Góp phần nâng cao độ tin cậy của dữ liệu số, giảm rủi ro sai lệch và tăng hiệu quả quản lý nhà nước trong môi trường điện tử. Đến năm 2027, hình thành và đưa vào vận hành sản phẩm đối với các nhóm hồ sơ điện tử ưu tiên; mở rộng phạm vi áp dụng theo lộ trình sau năm 2027 trên cơ sở kết quả đánh giá và mức độ sẵn sàng của các hệ thống nguồn.

b) SP2. Hệ thống xác minh văn bằng, chứng chỉ trên blockchain

Mục tiêu triển khai: Triển khai SP2 để xác minh tính hợp lệ của văn bằng, chứng chỉ do các cơ sở giáo dục, đào tạo thuộc phạm vi áp dụng phát hành. Sản phẩm này nhằm giảm rủi ro làm giả, sửa đổi hoặc sử dụng văn bằng, chứng chỉ không hợp lệ; đồng thời rút ngắn thời gian xác minh, tăng độ tin cậy trong khai thác, sử dụng và đối chiếu thông tin.

Phạm vi và đối tượng áp dụng: Giai đoạn đầu, SP2 áp dụng đối với một số nhóm văn bằng, chứng chỉ có dữ liệu tương đối rõ, có đầu mối quản lý cụ thể và có nhu cầu xác minh thường xuyên, ưu tiên các nhóm văn bằng, chứng chỉ thuộc hệ thống giáo dục quốc dân theo quy định tại Thông tư số 10/2026/TT-BGDĐT ngày 26/02/2026 của Bộ Giáo dục và Đào tạo. Đối tượng áp dụng gồm các cơ sở giáo dục đại học, cao đẳng, các trường và cơ sở giáo dục nghề nghiệp trên địa bàn thành phố; cơ quan quản lý nhà nước có liên quan; tổ chức, doanh nghiệp và cá nhân có nhu cầu xác minh theo quy định. Phạm vi mở rộng được thực hiện theo lộ trình, không triển khai đồng loạt ngay từ đầu.

Mô hình triển khai và thành phần chính: Dữ liệu văn bằng, chứng chỉ tiếp tục được quản lý tại hệ thống nguồn của cơ sở giáo dục, đào tạo hoặc đơn vị có thẩm quyền quản lý dữ liệu theo quy định của Thông tư số 10/2026/TT-BGDĐT. Nền tảng tích hợp của thành phố thực hiện kết nối theo cơ chế thống nhất. SP2 tiếp nhận thông tin cần xác minh, xử lý dữ liệu tham chiếu và ghi nhận bằng chứng xác minh lên DNC-Chain. DNC-Chain chỉ thực hiện vai trò lớp tin cậy số phục vụ xác minh, không thay thế cơ sở dữ liệu gốc và không lưu trữ đầy đủ toàn bộ nội dung văn bằng, chứng chỉ. Nội dung kỹ thuật chi tiết của sản phẩm được thuyết minh tại Phần B Phụ lục I kèm theo Đề án.

Quy trình vận hành chính: Khi văn bằng, chứng chỉ được cấp mới hoặc được cập nhật trạng thái theo quy định, dữ liệu cần xác minh được gửi từ hệ thống nguồn qua lớp

tích hợp. SP2 xử lý thông tin tham chiếu và ghi nhận bằng chứng xác minh lên DNC-Chain. Khi phát sinh yêu cầu kiểm tra, hệ thống thực hiện tra cứu và đối chiếu với bằng chứng đã được ghi nhận để xác định tính hợp lệ của văn bằng, chứng chỉ. Kết quả xác minh được sử dụng cho mục đích tra cứu, tuyển dụng, tiếp nhận hồ sơ, đối chiếu thông tin và các hoạt động quản lý liên quan.

Điều kiện triển khai: SP2 chỉ triển khai khi dữ liệu văn bằng, chứng chỉ đã được chuẩn hoá theo quy định tại Thông tư số 10/2026/TT-BGDĐT và các quy định chuyên ngành có liên quan; cơ sở giáo dục, đào tạo tham gia có hệ thống nguồn hoặc có khả năng cập nhật dữ liệu theo chuẩn thống nhất; cơ quan chủ trì sản phẩm, cơ quan chủ trì dữ liệu nguồn và đầu mối phối hợp được xác định rõ. Việc triển khai phải bảo đảm đúng quy định về quản lý văn bằng, chứng chỉ, BVĐLCN theo Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, ATTT và phân quyền khai thác dữ liệu.

Nhiệm vụ chủ yếu: Rà soát, lựa chọn phạm vi văn bằng, chứng chỉ đưa vào triển khai trên cơ sở Thông tư số 10/2026/TT-BGDĐT. Chuẩn hóa dữ liệu, mã định danh và trạng thái xác minh. Hoàn thiện cơ chế kết nối giữa cơ sở giáo dục, đào tạo, cơ quan quản lý và SP2. Tổ chức kiểm thử quy trình xác minh. Đánh giá thời gian xử lý, độ chính xác và khả năng khai thác thực tế. Hoàn thiện cơ chế vận hành, giám sát và mở rộng theo điều kiện.

Kết quả cần đạt: Hình thành được sản phẩm hỗ trợ xác minh văn bằng, chứng chỉ nhanh, tin cậy và có thể kiểm chứng độc lập. Rút ngắn thời gian xác minh. Tăng số lượt xác minh qua môi trường số. Góp phần nâng cao chất lượng quản lý dữ liệu văn bằng, chứng chỉ trên địa bàn thành phố. Theo chỉ tiêu đã dự kiến, thời gian xác minh văn bằng đến năm 2027 đạt mức không quá 01 ngày; số lượt xác minh đạt từ 25.000 lượt/năm và mở rộng lên từ 50.000 lượt/năm vào giai đoạn sau.

2. Tầng 2 (SP3, SP4)

Tầng 2 gồm 02 sản phẩm có nhu cầu thực tiễn rõ, nhưng yêu cầu cao hơn về dữ liệu, tích hợp, pháp lý chuyên ngành và tổ chức thực hiện. Đây là nhóm chưa triển khai ngay trong giai đoạn đầu, mà được tổ chức thực hiện trong giai đoạn 2028-2030 khi các điều kiện chuẩn bị đã đầy đủ và kết quả triển khai Tầng 1 đã được đánh giá. Việc đưa các sản phẩm này vào triển khai phải bảo đảm thận trọng, có phạm vi phù hợp và không vượt quá khả năng quản trị, tích hợp và kiểm soát của thành phố.

Bảng 8. Cơ quan chủ trì sản phẩm, cơ quan chủ trì dữ liệu nguồn và cơ quan phối hợp đối với Tầng 2

SP	Cơ quan chủ trì sản phẩm	Cơ quan chủ trì dữ liệu nguồn	Cơ quan phối hợp
SP3	Sở Khoa học và Công nghệ	Sở Xây dựng đối với dữ liệu hạ tầng đô thị, giao thông, công trình công cộng, cấp thoát nước; Sở Nông nghiệp và Môi trường đối với dữ liệu môi trường, biến đổi khí hậu, mực nước, cảnh báo thiên tai,..	Ủy ban nhân dân các phường, xã tại khu vực thí điểm; các đơn vị quản lý hạ tầng đô thị, giao thông, cấp thoát nước; các đơn vị quan trắc, môi trường, phòng, chống thiên tai; doanh nghiệp công nghệ và đơn vị cung cấp giải pháp Digital Twin
SP4	Sở Y tế	Các bệnh viện và cơ sở y tế trên địa bàn thành phố	Sở Khoa học và Công nghệ

a) SP3. Digital Twin tích hợp blockchain

Mục tiêu triển khai: Triển khai SP3 để hỗ trợ quản lý dữ liệu hạ tầng đô thị và môi trường trên cơ sở mô hình số, đồng thời bổ sung cơ chế ghi nhận và kiểm chứng đối với các sự kiện vòng đời quan trọng. Sản phẩm này phục vụ các yêu cầu về nghiệm thu, bảo trì, sửa chữa, cập nhật phiên bản dữ liệu và làm rõ trách nhiệm giữa các bên tham gia quản lý, vận hành và giám sát hạ tầng đô thị. SP3 không ghi nhận toàn bộ dữ liệu Digital Twin trên DNC-Chain, mà là bổ sung lớp tin cậy số đối với các sự kiện có ý nghĩa quản lý, gắn với định hướng phát triển đô thị thông minh của thành phố theo Kiến trúc tổng thể thành phố thông minh thành phố Đà Nẵng phiên bản 2.0 ban hành kèm Quyết định số 3405/QĐ-UBND của Ủy ban nhân dân thành phố Đà Nẵng.

Phạm vi và đối tượng áp dụng: SP3 áp dụng đối với một số khu vực, công trình, hạ tầng và dữ liệu môi trường được lựa chọn thí điểm, có nhu cầu quản lý vòng đời rõ và có khả năng tổ chức dữ liệu theo chuẩn phù hợp. Đối tượng áp dụng gồm cơ quan quản lý nhà nước về hạ tầng đô thị, giao thông, công trình công cộng, cấp thoát nước, môi trường, phòng, chống thiên tai; các đơn vị vận hành hạ tầng; đơn vị quan trắc; nhà thầu và các chủ thể có liên quan trong phạm vi được lựa chọn triển khai. Phạm vi thực hiện được xác định theo từng khu vực thí điểm, không triển khai đồng loạt trên toàn thành phố ngay từ đầu.

Mô hình triển khai và thành phần chính: Nền tảng Digital Twin tiếp tục thực hiện chức năng quản lý mô hình số, dữ liệu hạ tầng, dữ liệu môi trường và trạng thái vận hành của đối tượng được theo dõi; dữ liệu hạ tầng đô thị và dữ liệu môi trường được chuẩn hoá theo Khung kiến trúc dữ liệu quốc gia tại Quyết định số 2439/QĐ-TTg và Danh mục dữ liệu quan trọng, dữ liệu cốt lõi tại Quyết định số 20/2025/QĐ-TTg trong phạm vi áp dụng. SP3 thực hiện chức năng tiếp nhận các sự kiện quan trọng, xử lý dữ liệu tham chiếu và ghi nhận bằng chứng xác minh lên DNC-Chain. DNC-Chain không lưu dữ liệu cảm biến thô liên tục, không lưu toàn bộ mô hình số và không thay thế nền tảng Digital Twin; chỉ ghi nhận các sự kiện có ý nghĩa quản lý như nghiệm thu, bảo trì, sửa chữa, cập nhật

phiên bản dữ liệu hoặc các mốc cần kiểm chứng. Cách tổ chức này bảo đảm đúng vai trò của blockchain và phù hợp với nguyên tắc dữ liệu của Đề án.

Quy trình vận hành chính: Khi nền tảng Digital Twin phát sinh các sự kiện quản lý quan trọng, thông tin sự kiện được gửi qua cơ chế tích hợp thống nhất. SP3 tiếp nhận, chuẩn hoá dữ liệu tham chiếu và ghi nhận bằng chứng xác minh lên DNC-Chain. Khi có yêu cầu kiểm tra, đối chiếu hoặc giải quyết tranh chấp, hệ thống thực hiện tra cứu và kiểm chứng theo mốc sự kiện đã được ghi nhận. Kết quả xác minh được sử dụng phục vụ nghiệm thu, giám sát, hậu kiểm, quản lý lịch sử bảo trì và làm rõ trách nhiệm giữa các bên liên quan.

Điều kiện triển khai: SP3 chỉ triển khai khi dữ liệu hạ tầng đô thị, môi trường và dữ liệu vận hành tại khu vực thí điểm đã được chuẩn hoá ở mức cần thiết theo Khung kiến trúc dữ liệu quốc gia và Kiến trúc tổng thể thành phố thông minh thành phố Đà Nẵng; phạm vi công trình, đối tượng và khu vực triển khai được xác định rõ; cơ quan chủ trì sản phẩm, cơ quan chủ trì dữ liệu nguồn và các đơn vị phối hợp được phân công cụ thể. Nền tảng Digital Twin phải có khả năng tích hợp với hạ tầng số của thành phố. Quy trình nghiệm thu, bảo trì, sửa chữa và cập nhật dữ liệu phải đủ rõ để xác định các sự kiện cần ghi nhận và kiểm chứng. Các yêu cầu về ATTT, ANM và kiểm soát dữ liệu phải được rà soát trước khi triển khai.

Nhiệm vụ chủ yếu: Rà soát, lựa chọn khu vực, công trình và nhóm dữ liệu thí điểm. Chuẩn hoá dữ liệu hạ tầng, dữ liệu môi trường và các mốc sự kiện cần ghi nhận theo Khung kiến trúc dữ liệu quốc gia và Danh mục dữ liệu quan trọng, dữ liệu cốt lõi. Hoàn thiện cơ chế phối hợp giữa cơ quan quản lý, đơn vị vận hành, đơn vị quan trắc và nhà thầu. Hoàn thiện cơ chế tích hợp giữa nền tảng Digital Twin và SP3. Tổ chức thử nghiệm quy trình ghi nhận, kiểm chứng và tra cứu sự kiện. Đánh giá khả năng vận hành, giá trị hỗ trợ nghiệm thu, bảo trì, giám sát và xử lý tranh chấp. Hoàn thiện điều kiện để mở rộng theo lộ trình.

Kết quả cần đạt: Hình thành được sản phẩm hỗ trợ ghi nhận và kiểm chứng các sự kiện vòng đời quan trọng của hạ tầng đô thị và môi trường. Tăng khả năng hậu kiểm, đối chiếu trách nhiệm và lưu vết lịch sử vận hành. Hỗ trợ công tác nghiệm thu, bảo trì, sửa chữa và giám sát liên cơ quan trên cơ sở dữ liệu có thể kiểm chứng. Tạo tiền đề để từng bước hình thành lớp tin cậy dữ liệu phục vụ quản lý hạ tầng đô thị trong giai đoạn tiếp theo và phục vụ định hướng phát triển đô thị thông minh của thành phố.

b) SP4. Hệ thống xác minh hồ sơ y tế trên blockchain

Mục tiêu triển khai: Triển khai SP4 để hỗ trợ xác minh trạng thái hồ sơ y tế, tăng khả năng kiểm chứng dữ liệu giữa các cơ sở khám, chữa bệnh và hỗ trợ chia sẻ hồ sơ y tế theo cơ chế có kiểm soát. Sản phẩm này phục vụ các yêu cầu về đối soát, kiểm chứng, giải quyết tranh chấp, phát hiện bất thường và bảo đảm quyền của người bệnh trong quá trình sử dụng, chuyển tuyến và khai thác hồ sơ y tế. SP4 không ghi nhận hồ sơ y tế đầy đủ trên DNC-Chain, chỉ ghi nhận bằng chứng đối với các sự kiện y tế có ý nghĩa quản lý.

Phạm vi và đối tượng áp dụng: SP4 áp dụng đối với một số bệnh viện và cơ sở y tế trên địa bàn thành phố có đủ điều kiện về dữ liệu, hệ thống thông tin và tổ chức thực hiện. Đối tượng áp dụng gồm cơ sở khám, chữa bệnh tham gia hệ thống; cơ quan quản lý

y tế; người bệnh trong phạm vi được triển khai; và các tổ chức có nhu cầu xác minh, đối chiếu thông tin theo quy định. Phạm vi thực hiện được xác định theo lộ trình, ưu tiên triển khai trước ở các cơ sở có điều kiện dữ liệu và hạ tầng tốt hơn.

Mô hình triển khai và thành phần chính: Hồ sơ y tế tiếp tục được quản lý tại hệ thống nguồn của từng cơ sở khám, chữa bệnh theo pháp luật chuyên ngành về y tế và Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15. SP4 tiếp nhận các sự kiện y tế đã được lựa chọn theo danh mục cho phép, xử lý dữ liệu tham chiếu và ghi nhận bằng chứng xác minh lên DNC-Chain. DNC-Chain không ghi chẩn đoán, đơn thuốc, kết quả xét nghiệm hoặc dữ liệu cá nhân chi tiết; chỉ ghi nhận bằng chứng đối với các sự kiện có ý nghĩa quản lý như tiếp nhận, hoàn tất điều trị, chuyển viện hoặc các trạng thái hồ sơ cần kiểm chứng. Cách tổ chức này bảo đảm hỗ trợ xác minh và liên thông có kiểm soát nhưng không làm phát sinh hạ tầng dữ liệu y tế song song và tuân thủ nguyên tắc tối thiểu hoá dữ liệu cá nhân.

Quy trình vận hành chính: Khi hệ thống quản lý bệnh viện ghi nhận một sự kiện y tế thuộc phạm vi cho phép, thông tin cần xác minh được gửi qua cơ chế tích hợp thống nhất. SP4 tiếp nhận, chuẩn hoá dữ liệu tham chiếu và ghi nhận bằng chứng xác minh lên DNC-Chain. Khi có yêu cầu chia sẻ, đối chiếu hoặc kiểm tra, hệ thống thực hiện tra cứu và kiểm chứng sự kiện đã được ghi nhận để hỗ trợ liên thông hồ sơ có kiểm soát giữa các cơ sở y tế, phục vụ phát hiện bất thường và làm rõ trạng thái hồ sơ khi cần thiết. Kết quả xác minh được sử dụng theo thẩm quyền, đúng mục đích và phù hợp quy định về bảo vệ dữ liệu y tế.

Điều kiện triển khai: SP4 chỉ triển khai khi cơ sở khám, chữa bệnh tham gia có hệ thống nguồn đủ điều kiện tích hợp; dữ liệu hồ sơ y tế được chuẩn hoá ở mức cần thiết; danh mục sự kiện y tế được phép ghi nhận được xác định rõ; và cơ quan chủ trì, cơ quan dữ liệu nguồn, đầu mối phối hợp được phân công cụ thể. Việc triển khai phải tuân thủ chặt chẽ các quy định của pháp luật chuyên ngành về khám bệnh, chữa bệnh, Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, Luật Giao dịch điện tử số 20/2023/QH15, các quy định về ATTT, ANM và phân quyền khai thác dữ liệu y tế. Cơ chế chia sẻ và kiểm chứng hồ sơ phải gắn với sự đồng ý của người bệnh theo quy định về BVDLCN và đúng phạm vi pháp lý cho phép.

Nhiệm vụ chủ yếu: Lựa chọn cơ sở y tế và phạm vi hồ sơ phù hợp để triển khai. Chuẩn hoá dữ liệu, mã hồ sơ và danh mục sự kiện y tế cần ghi nhận. Hoàn thiện cơ chế phối hợp giữa Sở Y tế, cơ sở khám, chữa bệnh và đầu mối kỹ thuật. Hoàn thiện cơ chế tích hợp giữa hệ thống nguồn và SP4 bảo đảm nguyên tắc tối thiểu hoá dữ liệu cá nhân và cơ chế xin ý kiến, thu thập sự đồng ý của người bệnh theo Luật Bảo vệ dữ liệu cá nhân. Tổ chức thử nghiệm quy trình ghi nhận, xác minh và chia sẻ có kiểm soát. Đánh giá khả năng phát hiện sai lệch, bất thường và khả năng hỗ trợ đối soát giữa các cơ sở. Hoàn thiện điều kiện để mở rộng theo lộ trình.

Kết quả cần đạt: Hình thành được sản phẩm hỗ trợ xác minh trạng thái hồ sơ y tế, tăng khả năng liên thông có kiểm soát và hỗ trợ kiểm chứng giữa các cơ sở khám, chữa bệnh. Tăng khả năng phát hiện sai lệch, bất thường trong quá trình khai thác và sử dụng dữ liệu y tế. Hỗ trợ bảo vệ quyền của người bệnh khi cần chuyển tuyến, đối chiếu hoặc

xác minh thông tin theo đúng nguyên tắc BVDLCN. Tạo cơ sở thực tiễn để từng bước mở rộng kết nối với các hệ thống y tế quy mô lớn hơn trong giai đoạn tiếp theo.

3. Tầng 3 (SP5, SP6, SP7)

Tầng 3 gồm 03 sản phẩm phục vụ phát triển kinh tế dữ liệu, dịch vụ số và các mô hình khai thác dữ liệu trong môi trường số của thành phố, triển khai trong giai đoạn 2028-2030, khi hạ tầng dùng chung, cơ chế dữ liệu, điều kiện tích hợp và kết quả triển khai các tầng trước đã đủ cơ sở mở rộng. Việc tổ chức triển khai tuân thủ nguyên tắc: sử dụng blockchain để xác minh, kiểm chứng, truy vết và quản lý giao dịch dữ liệu, giao dịch dịch vụ số; không tổ chức theo hướng TSMH có tính chất tài chính, không hình thành sàn giao dịch tài chính số công khai và không vận hành như mô hình giao dịch TSMH công khai.

Bảng 9. Cơ quan chủ trì sản phẩm, cơ quan chủ trì dữ liệu nguồn và cơ quan phối hợp đối với Tầng 3

SP	Cơ quan chủ trì sản phẩm	Cơ quan chủ trì dữ liệu nguồn	Cơ quan phối hợp
SP5	Sở Khoa học và Công nghệ	Các cơ quan, đơn vị chủ quản dữ liệu được phép chia sẻ; Trung tâm dữ liệu thành phố	Văn phòng UBND thành phố; Công an thành phố; các doanh nghiệp công nghệ
SP6	Sở Khoa học và Công nghệ	Các chủ sở hữu tài sản sở hữu trí tuệ	Cục Sở hữu trí tuệ; Sở Tài chính; các trung tâm đổi mới sáng tạo
SP7	Sở Văn hoá, Thể thao và Du lịch	Các doanh nghiệp du lịch, dịch vụ tham gia; Sở Công Thương	Sở Khoa học và Công nghệ

a) SP5. Sàn giao dịch dữ liệu thành phố tích hợp blockchain

Mục tiêu triển khai: Triển khai SP5 để hỗ trợ niêm yết dữ liệu, cấp phép khai thác dữ liệu và ghi nhận giao dịch dữ liệu trong môi trường giao dịch điện tử có kiểm soát. Sản phẩm này nhằm xác minh nguồn gốc dữ liệu, điều kiện sử dụng, phạm vi khai thác và lịch sử giao dịch dữ liệu. SP5 phục vụ phát triển kinh tế dữ liệu của thành phố theo định hướng tại Luật Dữ liệu số 60/2024/QH15. SP5 không hình thành thị trường TSMH và không tổ chức giao dịch TSMH dưới bất kỳ hình thức nào.

Phạm vi và đối tượng áp dụng: SP5 áp dụng đối với các bộ dữ liệu, dịch vụ dữ liệu và nhu cầu khai thác dữ liệu được phép chia sẻ theo quy định của Luật Dữ liệu và Nghị định số 278/2025/NĐ-CP của Chính phủ về kết nối, chia sẻ dữ liệu bắt buộc; không áp dụng đối với dữ liệu thuộc Danh mục dữ liệu quan trọng, dữ liệu cốt lõi được quy định tại Quyết định số 20/2025/QĐ-TTg, trừ trường hợp có quyết định của cơ quan có thẩm quyền cho phép chia sẻ. Đối tượng áp dụng gồm cơ quan, đơn vị chủ quản dữ liệu; tổ chức, doanh nghiệp có nhu cầu khai thác dữ liệu; đơn vị quản lý hạ tầng dữ liệu của thành phố; và các cơ quan có thẩm quyền kiểm tra, giám sát việc chia sẻ, khai thác dữ liệu. Phạm vi triển khai thực hiện theo lộ trình, ưu tiên các bộ dữ liệu có nhu cầu khai thác rõ, có điều kiện pháp lý và có khả năng kiểm soát quyền sử dụng.

Mô hình triển khai và thành phần chính: Dữ liệu gốc tiếp tục được quản lý tại cơ quan, đơn vị chủ quản hoặc tại hệ thống dữ liệu của thành phố theo Luật Dữ liệu số 60/2024/QH15 và các quy định về quản trị dữ liệu. SP5 thực hiện chức năng niêm yết dữ liệu, công bố metadata, quản lý điều kiện khai thác, cấp quyền sử dụng và ghi nhận bằng chứng giao dịch dữ liệu trên DNC-Chain. DNC-Chain chỉ ghi nhận hồ sơ tham chiếu, trạng thái cấp phép và các mốc giao dịch; không ghi dữ liệu gốc trực tiếp lên chuỗi. Đối với các dữ liệu có yếu tố dữ liệu cá nhân, việc xử lý, chia sẻ và kiểm chứng phải tuân thủ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15. Cách tổ chức này bảo đảm đúng nguyên tắc dữ liệu của Đề án, đồng thời hình thành môi trường giao dịch dữ liệu minh bạch, có kiểm soát và có thể hậu kiểm.

Quy trình vận hành chính: Khi tổ chức hoặc doanh nghiệp đăng ký niêm yết dữ liệu, hệ thống tiếp nhận metadata, điều kiện khai thác và hồ sơ mô tả. Hệ thống thực hiện phân loại dữ liệu theo quy định tại Luật Dữ liệu và Quyết định số 20/2025/QĐ-TTg về Danh mục dữ liệu quan trọng, dữ liệu cốt lõi; kiểm tra điều kiện chia sẻ và ghi nhận hồ sơ tham chiếu lên DNC-Chain. Khi phát sinh giao dịch khai thác dữ liệu, hệ thống ghi nhận các sự kiện như cấp quyền truy cập, gia hạn, điều chỉnh, chấm dứt hoặc thu hồi quyền sử dụng. Quyền truy cập dữ liệu được kiểm soát theo phạm vi, thời hạn và mục đích đã được cấp phép. Lịch sử giao dịch và lịch sử khai thác được lưu vết để phục vụ giám sát, hậu kiểm và xử lý vi phạm khi cần thiết.

Điều kiện triển khai: SP5 chỉ triển khai khi danh mục dữ liệu được phép chia sẻ đã được xác định rõ theo Luật Dữ liệu, Nghị định số 278/2025/NĐ-CP và Quyết định số 20/2025/QĐ-TTg; cơ quan chủ quản dữ liệu, cơ quan chủ trì sản phẩm và đầu mối quản lý hạ tầng dữ liệu được phân công cụ thể. Dữ liệu phải được phân loại theo mức độ nhạy cảm, điều kiện chia sẻ và nguy cơ tái định danh; đối với dữ liệu cá nhân, phải tuân thủ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15. Cơ chế cấp phép khai thác, giới hạn mục đích sử dụng, giới hạn kết hợp dữ liệu và kiểm soát truy cập phải được thiết lập đầy đủ. Các yêu cầu về BVDLCN, ATTT, ANM và giám sát khai thác dữ liệu phải được rà soát trước khi đưa vào vận hành.

Nhiệm vụ chủ yếu: Rà soát, lựa chọn nhóm dữ liệu đủ điều kiện đưa vào niêm yết và khai thác theo quy định của Luật Dữ liệu và các văn bản hướng dẫn. Chuẩn hoá metadata, điều kiện sử dụng và cơ chế phân loại dữ liệu trên cơ sở Quyết định số 20/2025/QĐ-TTg. Hoàn thiện cơ chế phối hợp giữa cơ quan chủ quản dữ liệu, đơn vị vận hành hạ tầng và tổ chức khai thác dữ liệu. Hoàn thiện cơ chế cấp phép, gia hạn, điều chỉnh, thu hồi quyền truy cập. Tổ chức thử nghiệm quy trình niêm yết, cấp phép, khai thác và hậu kiểm. Đánh giá khả năng vận hành, giá trị hỗ trợ phát triển dịch vụ dữ liệu và mức độ đáp ứng yêu cầu quản lý. Hoàn thiện điều kiện để mở rộng theo lộ trình.

Kết quả cần đạt: Hình thành được sản phẩm hỗ trợ niêm yết dữ liệu, cấp phép khai thác dữ liệu và ghi nhận giao dịch dữ liệu trong môi trường giao dịch điện tử có kiểm soát. Tăng khả năng kiểm chứng nguồn gốc dữ liệu, điều kiện sử dụng và lịch sử giao dịch. Tạo điều kiện kết nối cung-cầu dữ liệu, hỗ trợ phát triển dịch vụ dữ liệu, ứng dụng trí tuệ nhân tạo và các mô hình đổi mới sáng tạo trên địa bàn thành phố; góp phần phát triển kinh tế dữ liệu theo định hướng quốc gia.

b) SP6. Sàn giao dịch tài sản sở hữu trí tuệ tích hợp blockchain

Mục tiêu triển khai: Triển khai SP6 để hỗ trợ đăng ký bằng chứng tham chiếu, xác minh trạng thái và hỗ trợ giao dịch khai thác tài sản sở hữu trí tuệ trong môi trường số. Sản phẩm này nhằm tăng khả năng tra cứu, kiểm chứng, truy vết và thương mại hoá tài sản sở hữu trí tuệ; đồng thời hỗ trợ kết nối giữa chủ sở hữu tài sản, đơn vị có nhu cầu khai thác và các chủ thể liên quan. Blockchain trong SP6 chỉ là lớp tin cậy số bổ sung, không thay thế thẩm quyền xác lập quyền, đăng ký quyền và quản lý nhà nước về sở hữu trí tuệ theo Luật Sở hữu trí tuệ.

Phạm vi và đối tượng áp dụng: SP6 áp dụng đối với tài sản sở hữu trí tuệ của viện nghiên cứu, cơ sở đào tạo, doanh nghiệp và cá nhân có nhu cầu đưa vào môi trường tra cứu, cấp phép hoặc khai thác thương mại hoá trên nền tảng số, trong phạm vi và theo điều kiện quy định tại Luật Sở hữu trí tuệ và các văn bản hướng dẫn thi hành. Đối tượng áp dụng gồm chủ sở hữu tài sản sở hữu trí tuệ, tổ chức có nhu cầu khai thác, đơn vị hỗ trợ đổi mới sáng tạo và các cơ quan, tổ chức có thẩm quyền tham gia tra cứu, kiểm chứng hoặc xác minh trạng thái pháp lý của tài sản. Phạm vi triển khai được mở rộng theo lộ trình, gắn với mức độ hoàn thiện của dữ liệu tham chiếu và cơ chế phối hợp giữa các bên.

Mô hình triển khai và thành phần chính: SP6 được tổ chức theo hướng ghi nhận bằng chứng thời gian, trạng thái tham chiếu và lịch sử khai thác của tài sản sở hữu trí tuệ trên DNC-Chain. Dữ liệu gốc, hồ sơ pháp lý và quyết định xác lập quyền tiếp tục do cơ quan nhà nước có thẩm quyền về sở hữu trí tuệ và chủ sở hữu tài sản quản lý theo Luật Sở hữu trí tuệ. DNC-Chain chỉ ghi nhận bằng chứng tham chiếu đối với các mốc quan trọng như hình thành tài sản, cấp văn bằng, cấp phép khai thác hoặc chuyển nhượng; không thay thế hệ thống đăng ký sở hữu trí tuệ quốc gia. Việc giao dịch trên nền tảng tuân thủ quy định pháp luật về giao dịch điện tử tại Luật Giao dịch điện tử số 20/2023/QH15. Phần thương mại của sản phẩm do doanh nghiệp đầu tư; ngân sách nhà nước chỉ đầu tư cho phần quản lý, tích hợp với DNC-Chain, giám sát tuân thủ và bảo đảm chức năng quản lý nhà nước.

Quy trình vận hành chính: Khi chủ sở hữu đăng ký bằng chứng sáng tạo hoặc đưa tài sản vào hệ thống, nền tảng tiếp nhận hồ sơ tham chiếu và ghi nhận bằng chứng thời gian lên DNC-Chain. Khi có quyết định cấp văn bằng hoặc thay đổi trạng thái pháp lý từ cơ quan nhà nước có thẩm quyền về sở hữu trí tuệ, hệ thống đồng bộ trạng thái từ nguồn chính thức và cập nhật trạng thái tham chiếu. Khi phát sinh giao dịch cấp phép khai thác hoặc chuyển nhượng theo quy định của Luật Sở hữu trí tuệ, các bên thực hiện xác nhận theo quy trình số; hệ thống ghi nhận các mốc giao dịch lên DNC-Chain để phục vụ tra cứu, đối chiếu và hậu kiểm. Việc ghi nhận trên chuỗi chỉ có giá trị tham chiếu bổ sung; các thủ tục pháp lý chính thức vẫn thực hiện theo quy định của pháp luật.

Điều kiện triển khai: SP6 chỉ triển khai khi tài sản sở hữu trí tuệ tham gia có chủ sở hữu rõ, trạng thái pháp lý rõ và hồ sơ dữ liệu tham chiếu có thể chuẩn hoá. Cơ quan chủ trì sản phẩm, chủ sở hữu tài sản và các đơn vị phối hợp phải được xác định cụ thể. Cơ chế xác minh danh tính, xác định tư cách pháp lý, cấp phép khai thác và ghi nhận giao dịch phải được thiết lập chặt chẽ. Việc triển khai phải tuân thủ Luật Sở hữu trí tuệ, Luật Giao

dịch điện tử số 20/2023/QH15, pháp luật về dữ liệu, ATTT và các quy định liên quan đến phân định đầu tư công - đầu tư thương mại.

Nhiệm vụ chủ yếu: Rà soát, lựa chọn nhóm tài sản sở hữu trí tuệ phù hợp để đưa vào thí điểm trên cơ sở Luật Sở hữu trí tuệ và các văn bản hướng dẫn. Chuẩn hoá dữ liệu tham chiếu, trạng thái văn bằng và thông tin khai thác. Hoàn thiện cơ chế phối hợp giữa chủ sở hữu tài sản, đơn vị hỗ trợ đổi mới sáng tạo, cơ quan chuyên môn về sở hữu trí tuệ và đơn vị vận hành nền tảng. Hoàn thiện cơ chế ghi nhận bằng chứng thời gian, đồng bộ trạng thái pháp lý và lưu vết giao dịch khai thác. Tổ chức thử nghiệm quy trình tra cứu, xác minh, cấp phép khai thác và hậu kiểm. Đánh giá khả năng hỗ trợ thương mại hoá, thẩm định và kết nối cung-cầu khai thác tài sản sở hữu trí tuệ.

Kết quả cần đạt: Hình thành được sản phẩm hỗ trợ tra cứu, kiểm chứng, cấp phép khai thác và truy vết lịch sử giao dịch của tài sản sở hữu trí tuệ trong môi trường giao dịch điện tử, bám sát khung pháp lý về sở hữu trí tuệ và giao dịch điện tử của quốc gia. Tăng khả năng kết nối giữa chủ sở hữu tài sản và tổ chức có nhu cầu khai thác. Hỗ trợ thương mại hoá kết quả nghiên cứu, sáng tạo trên cơ sở dữ liệu có thể kiểm chứng, minh bạch và có kiểm soát.

c) SP7. Chương trình khách hàng trung thành của thành phố (City Loyalty Program) tích hợp blockchain

Mục tiêu triển khai: Triển khai SP7 để hình thành chương trình điểm thưởng số dùng chung phục vụ hệ sinh thái du lịch, dịch vụ của thành phố. Sản phẩm này nhằm hỗ trợ tích điểm, đổi thưởng, liên thông ưu đãi giữa các doanh nghiệp tham gia; tăng trải nghiệm của người dân và du khách; đồng thời hỗ trợ thành phố hình thành dữ liệu tổng hợp phục vụ phân tích hành vi du lịch và hoạch định chính sách. Phạm vi của SP7 là chương trình điểm thưởng dịch vụ, không phải tài sản tài chính và không quy đổi sang tiền pháp định; không có chức năng thanh toán và không thuộc phạm vi điều chỉnh của pháp luật về thị trường TSMH.

Phạm vi và đối tượng áp dụng: SP7 áp dụng đối với mạng lưới doanh nghiệp du lịch, lưu trú, ẩm thực, tham quan, mua sắm và dịch vụ có nhu cầu tham gia chương trình khách hàng trung thành dùng chung của thành phố. Đối tượng áp dụng gồm doanh nghiệp tham gia chương trình, người dân, du khách sử dụng dịch vụ và cơ quan quản lý nhà nước có liên quan. Giai đoạn đầu ưu tiên triển khai theo phạm vi thí điểm phù hợp, sau đó mở rộng theo mức độ tham gia của doanh nghiệp và khả năng vận hành thực tế.

Mô hình triển khai và thành phần chính: SP7 được tổ chức như một nền tảng điểm thưởng số dùng chung, kết nối các doanh nghiệp cung cấp dịch vụ du lịch và dịch vụ liên quan thông qua cơ chế tích hợp thống nhất. DNC-Chain thực hiện chức năng ghi nhận sự kiện tích điểm, đổi thưởng và lưu vết lịch sử giao dịch điểm thưởng. DNC-Chain không thay thế hệ thống bán hàng, hệ thống quản trị khách hàng hoặc hệ thống thanh toán của doanh nghiệp. Điểm thưởng số của chương trình chỉ được sử dụng trong phạm vi chính sách ưu đãi, đổi thưởng và khai thác dịch vụ của hệ sinh thái tham gia; không giao dịch trên sàn, không chuyển thành tài sản tài chính và không quy đổi sang tiền pháp định. Việc xử lý dữ liệu cá nhân của người dùng trong chương trình tuân thủ Luật Bảo vệ dữ liệu cá

nhân số 91/2025/QH15. Phần quản lý, tích hợp và giám sát thuộc nhà nước bảo đảm; phần vận hành thương mại do doanh nghiệp đầu tư theo cơ chế phù hợp.

Quy trình vận hành chính: Khi người dùng sử dụng dịch vụ tại đơn vị tham gia, doanh nghiệp gửi sự kiện giao dịch lên hệ thống theo chuẩn chung. Hệ thống thực hiện đối soát với dữ liệu nguồn, ghi nhận sự kiện tích điểm hoặc đổi thưởng lên DNC-Chain và cập nhật số dư điểm của người dùng. Người dùng theo dõi điểm, tra cứu ưu đãi và thực hiện đổi thưởng thông qua ứng dụng phù hợp. Thành phố khai thác dữ liệu tổng hợp, đã được ẩn danh hoá theo nguyên tắc BVDLCN, để phục vụ quản lý và phân tích xu hướng tiêu dùng, thời gian lưu trú, hiệu quả kích cầu và các nội dung liên quan.

Điều kiện triển khai: SP7 chỉ triển khai khi xác định rõ phạm vi chương trình, cơ chế tích điểm, đổi thưởng, mạng lưới doanh nghiệp tham gia và cơ chế phân định rõ giữa phần quản lý nhà nước với phần vận hành thương mại. Doanh nghiệp tham gia phải có hệ thống nguồn đủ để ghi nhận giao dịch và kết nối với nền tảng dùng chung. Cơ chế xác minh người dùng, đối soát giao dịch, phòng chống gian lận, BVDLCN theo Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và bảo vệ quyền lợi người tiêu dùng phải được thiết lập đầy đủ trước khi vận hành. Việc triển khai phải tuân thủ chặt chẽ quy định pháp luật về dữ liệu, BVDLCN, giao dịch điện tử và các quy định liên quan.

Nhiệm vụ chủ yếu: Rà soát, lựa chọn phạm vi dịch vụ và doanh nghiệp tham gia giai đoạn đầu. Hoàn thiện cơ chế tích điểm, đổi thưởng và quy tắc vận hành chương trình. Hoàn thiện cơ chế tích hợp giữa doanh nghiệp tham gia và nền tảng dùng chung. Thiết lập cơ chế đối soát, giám sát giao dịch, kiểm soát gian lận, BVDLCN và ẩn danh hoá dữ liệu tổng hợp theo Luật Bảo vệ dữ liệu cá nhân. Tổ chức thử nghiệm trong phạm vi phù hợp. Đánh giá hiệu quả kích cầu, mức độ tham gia của doanh nghiệp, trải nghiệm của người dùng và khả năng hình thành dữ liệu tổng hợp phục vụ quản lý. Hoàn thiện điều kiện để mở rộng theo lộ trình.

Kết quả cần đạt: Hình thành được chương trình khách hàng trung thành dùng chung ở quy mô thành phố, hỗ trợ tích điểm và đổi thưởng giữa các dịch vụ tham gia. Tăng mức độ liên kết giữa các doanh nghiệp du lịch, dịch vụ. Hỗ trợ nâng cao trải nghiệm của người dân và du khách trên cơ sở bảo đảm quyền của chủ thể dữ liệu. Từng bước hình thành dữ liệu tổng hợp, đã được ẩn danh hoá, phục vụ quản lý, phân tích xu hướng và xây dựng chính sách kích cầu du lịch, dịch vụ của thành phố.

4. Tầng 4 (SP8, SP9, SP10)

Tầng 4 gồm các mô hình chuyên biệt có yếu tố tài chính số, TSMH hoặc giao dịch số, được triển khai theo pháp luật chuyên ngành, cơ chế sandbox hoặc cơ chế riêng gắn với IFC. Đây không phải là nhóm sản phẩm dùng chung của thành phố. Vai trò của Đề án là tiếp nhận, định vị, điều phối ở cấp địa phương; chuẩn bị điều kiện triển khai; xác lập cơ chế phối hợp; hỗ trợ tích hợp kỹ thuật; hỗ trợ giám sát, tuân thủ và quản trị rủi ro trong phạm vi thẩm quyền của thành phố.

Trong mọi trường hợp, DNC-Chain chỉ tham gia với vai trò hạ tầng tin cậy số dùng chung, hỗ trợ xác minh, kiểm chứng, truy vết, đối soát, tích hợp và quản trị rủi ro kỹ thuật khi phù hợp; không phải nền tảng giao dịch chính và không tổ chức giao dịch TSMH trên hạ tầng blockchain dùng chung của thành phố. Ngân sách nhà nước trong khuôn khổ Đề

án chỉ sử dụng cho phần quản lý, giám sát, tích hợp, tuân thủ, quản trị rủi ro và bảo đảm chức năng quản lý nhà nước; không đầu tư phần thương mại của các mô hình này.

Bảng 10. Cơ quan chủ trì sản phẩm, cơ quan chủ trì dữ liệu nguồn và cơ quan phối hợp đối với Tầng 4

SP	Cơ quan chủ trì sản phẩm	Cơ quan chủ trì dữ liệu nguồn	Cơ quan phối hợp
SP8	Sở Khoa học và Công nghệ	Doanh nghiệp vận hành nền tảng theo phạm vi sandbox tại Nghị quyết số 55/2024/NQ-HĐND	Sở Tài chính; Ngân hàng Nhà nước khu vực 9; Cơ quan điều hành IFC tại Đà Nẵng; Công an thành phố
SP9	Cơ quan điều hành IFC tại Đà Nẵng	Tổ chức phát hành và doanh nghiệp vận hành nền tảng theo cơ chế riêng tại Nghị định số 323/2025/NĐ-CP	Sở Tài chính; Ngân hàng Nhà nước khu vực 9; Sở Tư pháp; các doanh nghiệp công nghệ tài chính
SP10	Cơ quan điều hành IFC tại Đà Nẵng	Doanh nghiệp vận hành nền tảng theo cơ chế được cấp có thẩm quyền phê duyệt	Các trung tâm đổi mới sáng tạo; Sở Tài chính; các doanh nghiệp công nghệ tài chính khởi nghiệp

Ghi chú: (i) cột "Cơ quan chủ trì dữ liệu nguồn" tại Bảng 10 chỉ rõ chủ thể quản lý dữ liệu nghiệp vụ của từng sản phẩm Tầng 4, gồm doanh nghiệp vận hành nền tảng và tổ chức tham gia, hoạt động theo cơ chế riêng, pháp luật chuyên ngành và phạm vi được cơ quan có thẩm quyền cho phép; (ii) "Cơ quan điều hành IFC tại Đà Nẵng" là chủ thể quản lý và điều hành trực tiếp các hoạt động tại IFC trên địa bàn theo Khoản 3 Điều 10 Nghị định số 323/2025/NĐ-CP.

a) SP8. Nền tảng chuyển đổi TSMH sang tiền pháp định

Mục tiêu triển khai: Đề án không cấp sandbox mới cho SP8 và không thay thế cơ chế thử nghiệm hiện hành. Tiếp tục theo dõi, đánh giá và điều phối việc triển khai SP8 trong 02 phạm vi: (i) trong cơ chế sandbox đã được thiết lập theo Nghị quyết số 55/2024/NQ-HĐND ngày 13/12/2024 của Hội đồng nhân dân thành phố Đà Nẵng và Quyết định số 1181/QĐ-UBND ngày 26/8/2025 của Ủy ban nhân dân thành phố Đà Nẵng về việc phê duyệt phương án sandbox đối với mô hình chuyển đổi TSMH; (ii) ngoài sandbox, theo pháp luật chuyên ngành về thị trường TSMH tại thời điểm triển khai, gồm Nghị quyết số 05/2025/NQ-CP ngày 09/9/2025 của Chính phủ về triển khai thí điểm thị trường tài sản mã hoá tại Việt Nam và các văn bản pháp luật chuyên ngành có liên quan. Sản phẩm này phục vụ nhu cầu chuyển đổi TSMH sang đồng Việt Nam trong phạm vi cho phép, đồng thời tạo dữ liệu thực tiễn để cơ quan quản lý đánh giá mức độ phù hợp của mô hình, yêu cầu tuân thủ và khả năng kiểm soát rủi ro. SP8 không cấu thành phương tiện thanh toán mới và không thay thế các phương tiện thanh toán hợp pháp theo Nghị định số 52/2024/NĐ-CP của Chính phủ về thanh toán không dùng tiền mặt.

Phạm vi và đối tượng áp dụng: SP8 được tiếp tục triển khai trong phạm vi cơ chế sandbox đã được phê duyệt. Đối tượng tham gia gồm doanh nghiệp vận hành nền tảng, cơ quan quản lý nhà nước có liên quan, các điểm chấp nhận thanh toán trong phạm vi được

phép và người dùng thuộc phạm vi thử nghiệm. Việc mở rộng phạm vi chỉ được xem xét theo từng bước, trên cơ sở kết quả vận hành, yêu cầu tuân thủ pháp luật, yêu cầu kiểm soát rủi ro và quyết định của cơ quan có thẩm quyền.

Mô hình triển khai và thành phần chính: Doanh nghiệp vận hành chịu trách nhiệm phát triển và vận hành nền tảng nghiệp vụ theo mô hình đã được phê duyệt trong sandbox. Nền tảng này thực hiện đăng ký tài khoản, xác minh danh tính điện tử, tiếp nhận giao dịch và tổ chức chuyển đổi theo phạm vi được phép; hợp đồng thông minh phục vụ chuyển đổi phải thiết lập cơ chế phân loại giao dịch theo quy mô (theo nguyên tắc tương đương Thông tư số 50/2024/TT-NHNN của Ngân hàng Nhà nước về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng) và áp dụng các hình thức xác nhận giao dịch tương ứng (mật khẩu, OTP, sinh trắc học qua VNeID Mức 2, chữ ký số) phù hợp với từng nhóm quy mô nhằm phòng, chống gian lận, lừa đảo; hoạt động kế toán đối với các tổ chức tham gia tuân thủ Thông tư số 15/2026/TT-BTC ngày 04/3/2026 của Bộ Tài chính hướng dẫn nguyên tắc kế toán đối với các tổ chức tham gia thị trường tài sản mã hoá tại Việt Nam. DNC-Chain không tham gia vào luồng giao dịch người dùng cuối và không tiếp nhận chi tiết giao dịch cá nhân, số dư tài khoản hoặc dữ liệu người dùng. DNC-Chain chỉ ghi nhận lớp dữ liệu giám sát, dữ liệu đối soát, trạng thái cảnh báo, mã tham chiếu giao dịch và bằng chứng tuân thủ phục vụ lưu vết, truy vết, thanh tra, kiểm tra và hậu kiểm. Cách tổ chức này giữ đúng vai trò của DNC-Chain và đúng bản chất của SP8 là mô hình chuyên biệt theo sandbox có trước.

Quy trình vận hành chính: Người dùng thực hiện giao dịch trên nền tảng vận hành độc lập của doanh nghiệp theo cơ chế đã được phê duyệt. Nền tảng vận hành thực hiện xác minh danh tính, kiểm soát tuân thủ và xử lý giao dịch theo quy trình nghiệp vụ riêng. Định kỳ hoặc theo sự kiện giám sát, doanh nghiệp gửi báo cáo tuân thủ, dữ liệu tổng hợp theo ngưỡng, trạng thái KYC tổng thể, mã tham chiếu giao dịch và trạng thái cảnh báo cần thiết lên DNC-Chain. Cơ quan quản lý khai thác dữ liệu tổng hợp, dữ liệu giám sát và dữ liệu truy vết để phục vụ theo dõi, đánh giá, kiểm tra và xử lý rủi ro theo thẩm quyền.

Điều kiện triển khai: SP8 chỉ tiếp tục triển khai trong phạm vi sandbox đã được phê duyệt theo Nghị quyết số 55/2024/NQ-HĐND, giới hạn về không gian theo Khoản 1 Điều 1 của Nghị quyết này; việc triển khai SP8 ngoài phạm vi không gian này phải có quyết định của cơ quan có thẩm quyền cấp trung ương và khi doanh nghiệp vận hành tiếp tục đáp ứng đầy đủ các yêu cầu về KYC, AML/CFT, giám sát giao dịch, bảo vệ dữ liệu người dùng, lưu vết giao dịch, báo cáo phục vụ cơ quan quản lý và các yêu cầu kế toán theo Thông tư số 15/2026/TT-BTC. Cơ chế phối hợp giữa **Sở Khoa học và Công nghệ, Sở Tài chính, Ngân hàng Nhà nước khu vực 9**, doanh nghiệp vận hành và các cơ quan liên quan phải được duy trì rõ ràng. Việc xem xét mở rộng phạm vi chỉ thực hiện khi đã có đủ dữ liệu vận hành thực tế, phù hợp với định hướng triển khai thị trường tài sản mã hoá tại Việt Nam.

Nhiệm vụ chủ yếu: Tiếp tục theo dõi kết quả vận hành sandbox theo Nghị quyết số 55/2024/NQ-HĐND. Tổng hợp dữ liệu thực tiễn về người dùng, giao dịch, thời gian xử lý, tuân thủ và rủi ro. Hoàn thiện cơ chế phối hợp giữa cơ quan quản lý và doanh nghiệp vận hành. Hoàn thiện cơ chế tích hợp lớp giám sát, đối soát và truy vết với DNC-Chain. Bảo đảm thực hiện các yêu cầu kế toán theo Thông tư số 15/2026/TT-BTC đối với các tổ

chức tham gia. Đánh giá định kỳ về hiệu quả, mức độ tuân thủ và khả năng kiểm soát rủi ro. Xem xét phạm vi mở rộng theo từng bước khi đủ điều kiện

Kết quả cần đạt: Duy trì được cơ chế theo dõi, giám sát và đánh giá SP8 trong khuôn khổ sandbox đã được thiết lập. Tăng khả năng khai thác dữ liệu giám sát, đối soát và truy vết phục vụ quản lý nhà nước. Tạo cơ sở thực tiễn để xem xét khả năng hoàn thiện, điều chỉnh hoặc mở rộng mô hình theo cơ chế riêng trong giai đoạn tiếp theo, phù hợp với khung pháp lý quốc gia về thị trường TSMH.

b) SP9. Nền tảng phát hành, lưu ký và giao dịch TSMH có tài sản bảo đảm trong thế giới thực (Real World Assets - RWA)

Mục tiêu triển khai: Tổ chức điều kiện để triển khai SP9 như một nền tảng nghiệp vụ chuyên biệt phục vụ phát hành, lưu ký và giao dịch TSMH có tài sản tham chiếu trong khuôn khổ cơ chế riêng gắn với Trung tâm tài chính quốc tế theo Nghị quyết số 222/2025/QH15 ngày 27/6/2025 của Quốc hội về Trung tâm tài chính quốc tế tại Việt Nam và Nghị định số 323/2025/NĐ-CP ngày 18/12/2025 của Chính phủ về thành lập Trung tâm tài chính quốc tế tại Việt Nam. Sản phẩm này nhằm hỗ trợ doanh nghiệp, tổ chức có nhu cầu phát hành và giao dịch TSMH có tài sản tham chiếu theo cơ chế có kiểm soát; đồng thời hỗ trợ cơ quan quản lý nâng cao năng lực giám sát, đối soát, truy vết và quản trị rủi ro đối với nhóm mô hình tài chính số chuyên biệt. SP9 không phải sản phẩm dùng chung của thành phố.

Phạm vi và đối tượng áp dụng: SP9 áp dụng đối với các doanh nghiệp, tổ chức có nhu cầu phát hành TSMH có tài sản tham chiếu trong phạm vi pháp luật cho phép và theo cơ chế riêng gắn với IFC. Đối tượng tham gia gồm Cơ quan điều hành IFC tại Đà Nẵng, cơ quan tài chính, cơ quan tiền tệ, cơ quan tư pháp, tổ chức phát hành, nhà đầu tư thuộc phạm vi được phép và các doanh nghiệp công nghệ tài chính tham gia vận hành nền tảng. Phạm vi triển khai phải được xác định theo cơ chế sandbox hoặc cơ chế chuyên biệt do cơ quan có thẩm quyền quyết định, phù hợp với Nghị quyết số 05/2025/NQ-CP về thí điểm thị trường tài sản mã hoá tại Việt Nam.

Mô hình triển khai và thành phần chính: SP9 được tổ chức như một nền tảng nghiệp vụ phát hành, lưu ký và giao dịch TSMH có tài sản tham chiếu, hoạt động trong khuôn khổ cơ chế riêng gắn với Trung tâm tài chính quốc tế theo Nghị định số 323/2025/NĐ-CP. Nền tảng này có thể vận hành trên kiến trúc kỹ thuật hoặc blockchain phù hợp với mô hình triển khai cụ thể; không bắt buộc toàn bộ nghiệp vụ phải chạy trực tiếp trên DNC-Chain. Hồ sơ pháp lý của tài sản gốc, quyền sở hữu và quyền tài sản liên quan vẫn được quản lý theo pháp luật chuyên ngành và tại các hệ thống nguồn phù hợp; hoạt động kế toán của tổ chức tham gia tuân thủ Thông tư số 15/2026/TT-BTC. DNC-Chain chỉ thực hiện vai trò lớp giám sát, đối soát, lưu vết, báo cáo và truy vết trên chuỗi phục vụ quản lý nhà nước, thanh tra, kiểm tra và hậu kiểm. DNC-Chain không phải là nền tảng giao dịch chính của SP9.

Quy trình vận hành chính: Sau khi tổ chức phát hành được cơ quan có thẩm quyền cho phép theo cơ chế riêng gắn với IFC, nền tảng nghiệp vụ thực hiện phát hành, lưu ký và quản lý vòng đời giao dịch TSMH có tài sản tham chiếu theo cơ chế được phê duyệt. Các chức năng xác minh danh tính, phân loại nhà đầu tư, lưu ký tài sản, giám sát

AML/CFT, cảnh báo rủi ro và xử lý tình huống khẩn cấp được thực hiện trong nền tảng nghiệp vụ chuyên biệt. DNC-Chain tiếp nhận lớp dữ liệu giám sát, mã tham chiếu giao dịch, trạng thái cảnh báo, dữ liệu đối soát và bằng chứng cần thiết để hỗ trợ cơ quan quản lý theo dõi, kiểm tra và hậu kiểm. Hồ sơ pháp lý của tài sản gốc không ghi trực tiếp lên chuỗi; chỉ ghi nhận giá trị băm và dữ liệu tham chiếu cần thiết phục vụ kiểm chứng.

Điều kiện triển khai: SP9 chỉ triển khai khi có căn cứ pháp lý đầy đủ đối với tài sản gốc, quyền sở hữu và quyền tài sản liên quan; có cơ chế riêng gắn với Trung tâm tài chính quốc tế theo Nghị quyết số 222/2025/QH15 và Nghị định số 323/2025/NĐ-CP hoặc cơ chế sandbox được cơ quan có thẩm quyền cho phép; có cơ quan chủ trì sản phẩm, cơ quan phối hợp và doanh nghiệp vận hành được xác định rõ. Cơ chế xác minh danh tính, phân loại nhà đầu tư, lưu ký tài sản, giám sát AML/CFT, đối soát giao dịch, xử lý tình huống khẩn cấp và kế toán theo Thông tư số 15/2026/TT-BTC phải được thiết lập đầy đủ. Việc triển khai phải bảo đảm phân định rõ giữa phần đầu tư thương mại của doanh nghiệp và phần quản lý của nhà nước.

Nhiệm vụ chủ yếu: Rà soát điều kiện pháp lý và cơ chế chuyên biệt đối với tài sản tham chiếu theo pháp luật hiện hành về sở hữu, giao dịch tài sản và cơ chế IFC. Xác định rõ cơ quan chủ trì, cơ quan phối hợp và trách nhiệm của doanh nghiệp vận hành trong khuôn khổ Nghị định số 323/2025/NĐ-CP và các văn bản có liên quan. Hoàn thiện điều kiện tích hợp lớp giám sát, đối soát, lưu vết và truy vết với DNC-Chain. Hoàn thiện cơ chế phối hợp giữa cơ quan điều hành IFC tại Đà Nẵng, cơ quan tài chính, cơ quan tiền tệ, cơ quan tư pháp và doanh nghiệp công nghệ tài chính. Tổ chức theo dõi, đánh giá việc triển khai theo cơ chế được phê duyệt. Hoàn thiện điều kiện quản trị rủi ro, giám sát và hậu kiểm trong toàn bộ vòng đời vận hành.

Kết quả cần đạt: Hình thành được khuôn khổ điều phối, phối hợp và giám sát ở cấp địa phương đối với mô hình phát hành, lưu ký và giao dịch TSMH có tài sản tham chiếu trong không gian chuyên biệt gắn với Trung tâm tài chính quốc tế tại Đà Nẵng theo đúng Nghị quyết số 222/2025/QH15 và Nghị định số 323/2025/NĐ-CP. Tăng khả năng kiểm chứng, đối soát, lưu vết và truy vết giao dịch phục vụ quản lý nhà nước. Tạo điều kiện để thành phố từng bước hình thành năng lực tiếp cận, giám sát và quản trị rủi ro đối với mô hình RWA trong phạm vi được pháp luật cho phép.

c) SP10. Nền tảng gọi vốn cộng đồng trên blockchain

Mục tiêu triển khai: Tổ chức điều kiện để triển khai SP10 như một nền tảng gọi vốn cộng đồng có kiểm soát phục vụ các dự án khởi nghiệp sáng tạo và các mô hình phù hợp trong không gian chuyên biệt gắn với Trung tâm tài chính quốc tế theo Nghị quyết số 222/2025/QH15 và Nghị định số 323/2025/NĐ-CP. Sản phẩm này nhằm tăng tính minh bạch của cam kết góp vốn, đăng ký mua phần vốn, đăng ký mua chứng chỉ hoặc các hình thức tương đương được pháp luật chuyên ngành cho phép, hỗ trợ giám sát giải ngân theo từng mốc và tăng khả năng bảo vệ nhà đầu tư khi phát sinh rủi ro. SP10 không phải sản phẩm dùng chung của thành phố và không áp dụng mặc định cho mọi hình thức gọi vốn. Đối với các mô hình có liên quan tài sản số, TSMH, giao dịch số hoặc phân chia lợi ích tài chính, việc triển khai chỉ xem xét trong phạm vi pháp luật hiện hành, cơ chế sandbox theo Nghị quyết số 55/2024/NQ-HĐND của Hội đồng nhân dân thành phố hoặc theo

quyết định của cơ quan có thẩm quyền. Đối với các mô hình SP10 có liên quan đến hoạt động cung cấp dịch vụ về chứng khoán, việc triển khai bắt buộc phải được Ủy ban Chứng khoán Nhà nước chấp thuận theo Khoản 4 Điều 12 Luật Chứng khoán số 54/2019/QH14 (sửa đổi, bổ sung bởi Luật số 56/2024/QH15); Cơ quan điều hành IFC tại Đà Nẵng chủ trì phối hợp với Sở Tài chính, Ngân hàng Nhà nước khu vực 9 hướng dẫn doanh nghiệp vận hành tuân thủ thủ tục cấp phép, chấp thuận của Ủy ban Chứng khoán Nhà nước trước khi đưa vào vận hành.

Phạm vi và đối tượng áp dụng: SP10 áp dụng đối với các dự án khởi nghiệp sáng tạo, doanh nghiệp nhỏ và vừa và các mô hình gọi vốn cộng đồng phù hợp với cơ chế cho phép. Đối tượng tham gia gồm cơ quan điều hành IFC tại Đà Nẵng, các trung tâm đổi mới sáng tạo, doanh nghiệp vận hành nền tảng, nhà đầu tư hoặc cộng đồng tham gia theo phạm vi được phép và các cơ quan có thẩm quyền giám sát. Phạm vi triển khai phải được xác định theo từng mô hình, từng dự án và từng giai đoạn, không triển khai đại trà ngoài phạm vi cơ chế được phê duyệt.

Mô hình triển khai và thành phần chính: SP10 được tổ chức như một nền tảng gọi vốn cộng đồng có kiểm soát, do doanh nghiệp hoặc tổ chức phù hợp phát triển và vận hành trên kiến trúc kỹ thuật hoặc blockchain phù hợp với từng sản phẩm, từng dự án, trong khuôn khổ cơ chế riêng gắn với Trung tâm tài chính quốc tế hoặc cơ chế sandbox theo Nghị quyết số 55/2024/NQ-HĐND. Blockchain không thay thế quy trình thẩm định dự án, phê duyệt gọi vốn hoặc giám sát của cơ quan quản lý. DNC-Chain không tiếp nhận dữ liệu chi tiết của nhà đầu tư, số dư tài khoản hoặc toàn bộ dữ liệu vận hành của nền tảng. DNC-Chain chỉ thực hiện chức năng ghi nhận bằng chứng xác minh, dữ liệu giám sát, trạng thái giải ngân, trạng thái cảnh báo, dữ liệu đối soát và dữ liệu truy vết giao dịch ở lớp giám sát trên chuỗi khi có yêu cầu quản lý, giám sát và hậu kiểm.

Quy trình vận hành chính: Sau khi dự án được thẩm định và được phép mở gọi vốn theo cơ chế phù hợp, hồ sơ pháp lý của dự án được lưu tại hệ thống nguồn hoặc nền tảng nghiệp vụ; DNC-Chain chỉ ghi nhận giá trị băm tham chiếu và bằng chứng xác minh cần thiết. Khi nhà đầu tư hoặc người tham gia thực hiện cam kết góp vốn, nền tảng ghi nhận mã tham chiếu giao dịch, giá trị cam kết, trạng thái xử lý và dữ liệu giám sát cần thiết. Mỗi đợt giải ngân chỉ được thực hiện sau khi mốc tương ứng được xác nhận theo thẩm quyền. Các trạng thái giải ngân, trạng thái cảnh báo, dữ liệu đối soát và sự kiện kiểm soát cần thiết được ghi nhận trên DNC-Chain để phục vụ giám sát, truy vết, kiểm tra, kiểm toán và hậu kiểm.

Điều kiện triển khai: SP10 chỉ triển khai khi dự án, mô hình gọi vốn và cơ chế tham gia đã được xác định rõ; cơ quan chủ trì sản phẩm, cơ quan phối hợp và doanh nghiệp vận hành nền tảng được phân công cụ thể; cơ chế thẩm định dự án, cơ chế xác nhận mốc giải ngân, cơ chế kiểm soát cảnh báo và cơ chế dừng khẩn cấp đã được thiết lập đầy đủ. Việc triển khai phải phù hợp với pháp luật hiện hành, Nghị quyết số 222/2025/QH15 và Nghị định số 323/2025/NĐ-CP về IFC, hoặc cơ chế sandbox theo Nghị quyết số 55/2024/NQ-HĐND của Hội đồng nhân dân thành phố Đà Nẵng (giới hạn về không gian theo Khoản 1 Điều 1 của Nghị quyết này); đồng thời bảo đảm yêu cầu giám sát AML/CFT, lưu vết giao dịch, kiểm tra, thanh tra và hậu kiểm.

Nhiệm vụ chủ yếu: Rà soát cơ chế pháp lý và phạm vi gọi vốn được phép áp dụng theo Nghị quyết số 222/2025/QH15, Nghị định số 323/2025/NĐ-CP và Nghị quyết số 55/2024/NQ-HĐND. Xác định rõ mô hình, dự án và nhóm đối tượng tham gia. Hoàn thiện cơ chế phối hợp giữa Cơ quan điều hành IFC tại Đà Nẵng, trung tâm đổi mới sáng tạo, Sở Tài chính, doanh nghiệp vận hành nền tảng và các cơ quan có liên quan. Hoàn thiện điều kiện tích hợp lớp giám sát, đối soát, lưu vết và truy vết với DNC-Chain. Tổ chức theo dõi, đánh giá việc triển khai trong phạm vi cơ chế được phê duyệt. Hoàn thiện điều kiện kiểm soát rủi ro, bảo vệ nhà đầu tư và hậu kiểm đối với từng dự án, từng đợt gọi vốn.

Kết quả cần đạt: Hình thành được khuôn khổ điều phối, phối hợp và giám sát ở cấp địa phương đối với nền tảng gọi vốn cộng đồng có kiểm soát trong không gian chuyên biệt gắn với IFC Việt Nam tại Đà Nẵng, bám sát khung pháp lý quốc gia và cơ chế đặc thù của thành phố. Tăng khả năng ghi nhận cam kết góp vốn, giám sát giải ngân theo từng mốc, lưu vết và truy vết giao dịch phục vụ quản lý nhà nước. Tạo thêm dữ liệu thực tiễn để đánh giá nhu cầu thị trường, khả năng đáp ứng của cơ chế kiểm soát và hiệu quả của mô hình giám sát, đối soát, truy vết trong thực tế.

IV. VỀ CHUẨN HÓA DỮ LIỆU, TÍCH HỢP, AN TOÀN THÔNG TIN, AN NINH MẠNG

1. Chuẩn hoá dữ liệu và xác định phạm vi dữ liệu đưa vào sử dụng

Tổ chức rà soát, đánh giá mức độ sẵn sàng của dữ liệu nguồn theo từng nhóm sản phẩm, từng hệ thống và từng cơ quan, đơn vị tham gia. Nội dung rà soát tập trung vào mức độ đầy đủ, chính xác, đồng bộ, cập nhật, khả năng chia sẻ, khả năng tích hợp và khả năng truy xuất của dữ liệu. Trên cơ sở đó, xây dựng kế hoạch chuẩn hóa dữ liệu, siêu dữ liệu, mã tham chiếu và nhật ký trạng thái phục vụ xác minh, kiểm chứng, truy vết và đối soát.

Việc xác định phạm vi dữ liệu sử dụng phải phân định rõ giữa dữ liệu nguồn, dữ liệu ngoài chuỗi và dữ liệu ghi nhận trên chuỗi, thực hiện theo nguyên tắc đã xác định tại Khoản 1 Mục II Chương III. Dữ liệu nghiệp vụ tiếp tục được lưu trữ, cập nhật và quản lý tại hệ thống nguồn; DNC-Chain chỉ ghi nhận bằng chứng xác minh, dữ liệu tham chiếu và **dữ liệu tối thiểu cần thiết** phục vụ xác minh, đối soát, truy vết và hậu kiểm.

Cơ quan quản lý hệ thống nguồn chịu trách nhiệm về tính hợp pháp, đầy đủ, chính xác và cập nhật của dữ liệu nghiệp vụ. Đơn vị vận hành DNC-Chain chịu trách nhiệm về việc ghi nhận, lưu vết, kiểm chứng và bảo đảm toàn vẹn đối với dữ liệu xác minh trên chuỗi. Kết quả đánh giá mức độ sẵn sàng dữ liệu là căn cứ để xem xét cho phép tích hợp, thử nghiệm, vận hành hoặc mở rộng ứng dụng trong từng giai đoạn.

2. Bảo đảm chất lượng, đối soát và xử lý sai lệch dữ liệu trong tích hợp

Trên cơ sở bộ tiêu chuẩn, yêu cầu kết nối, chia sẻ và kiểm chứng dữ liệu đã được xác lập tại Khoản 3 Mục I Chương này, thành phố tổ chức các nhiệm vụ bảo đảm chất lượng dữ liệu, đối soát và xử lý sai lệch giữa các hệ thống tham gia tích hợp với DNC-Chain.

Đối với từng hệ thống và từng sản phẩm, phải xác định rõ phương thức truyền nhận dữ liệu, cách thức xác minh giao dịch, phương thức ghi dấu thời gian, cơ chế lưu vết và cách đối soát trạng thái giữa các hệ thống. Quy trình kỹ thuật phải được tổ chức đồng bộ với quy trình nghiệp vụ, bảo đảm dữ liệu được xác minh, đối chiếu và truy xuất đúng theo trách nhiệm xử lý của từng cơ quan, đơn vị tham gia. Không để xảy ra tình trạng dữ liệu được xác minh về mặt kỹ thuật nhưng không khớp với trạng thái xử lý thực tế tại hệ thống nguồn, hoặc ngược lại.

Tổ chức thực hiện việc kiểm chứng độc lập, tra cứu, truy xuất và hậu kiểm đối với các giao dịch, trạng thái và bằng chứng xác minh được ghi nhận trên DNC-Chain. Hoạt động kiểm chứng phải cho phép theo dõi quá trình xử lý của từng hồ sơ, đối chiếu trạng thái giữa các hệ thống liên quan, làm rõ trách nhiệm khi phát sinh sai lệch hoặc tranh chấp. Kết quả kiểm chứng được sử dụng phục vụ quản lý nhà nước, giải quyết khiếu nại, thanh tra, kiểm toán và các tình huống hậu kiểm khác theo quy định.

Đối với dữ liệu được tích hợp qua LGSP và các đầu mối chia sẻ dữ liệu khác, việc đối soát phải bảo đảm tính thống nhất giữa dữ liệu tại hệ thống nguồn, dữ liệu được chia sẻ qua nền tảng tích hợp và bằng chứng ghi nhận trên DNC-Chain. Trường hợp phát sinh sai lệch, cơ quan chủ trì hệ thống nguồn có trách nhiệm xác minh, điều chỉnh tại hệ thống nguồn; việc cập nhật trạng thái trên DNC-Chain được thực hiện theo đúng quy định đã phê duyệt, không ghi đè bản ghi cũ mà bổ sung bản ghi mới kèm lý do và căn cứ điều chỉnh, bảo đảm tính toàn vẹn của chuỗi sự kiện trong toàn bộ vòng đời hồ sơ.

3. Bảo đảm ATTT, ANM và BVDLCN

Trên cơ sở Quy chế bảo đảm ATTT, ANM và BVDLCN đã ban hành tại Khoản 5 Mục I Chương này, thành phố tổ chức các biện pháp cụ thể lồng ghép trong toàn bộ vòng đời triển khai DNC-Chain và các ứng dụng kết nối, từ khâu thiết kế, tích hợp, thử nghiệm, vận hành đến mở rộng.

Các biện pháp bảo đảm an toàn và bảo vệ dữ liệu phải được tổ chức đồng bộ, bao gồm kiểm soát truy cập, phân quyền theo chức năng, quản lý định danh kỹ thuật, quản lý khoá mật mã, mã hoá thông tin cần thiết, lưu vết truy cập, giám sát giao dịch và phát hiện bất thường.

Tổ chức thẩm định an toàn, an ninh và rà soát tuân thủ trước khi cho phép kết nối ứng dụng mới với DNC-Chain hoặc mở rộng phạm vi khai thác dữ liệu. Nội dung rà soát phải làm rõ loại dữ liệu sử dụng, mức độ nhạy cảm của dữ liệu, biện pháp bảo vệ, cơ chế lưu vết, phương án xử lý rủi ro và trách nhiệm của từng tổ chức tham gia. Đồng thời, duy trì cơ chế kiểm tra định kỳ, cảnh báo sớm, ứng cứu sự cố và xử lý vi phạm trong suốt quá trình vận hành.

Yêu cầu kỹ thuật được thuyết minh tại Phần A, Phụ lục I kèm theo Đề án.

4. Tổ chức kiểm tra, đánh giá, kiểm soát tuân thủ trong quá trình vận hành

Tổ chức kiểm tra, đánh giá và kiểm soát tuân thủ đối với DNC-Chain và các ứng dụng kết nối theo Quy chế quản trị, vận hành DNC-Chain tại Khoản 2 và Quy chế bảo đảm ATTT, ANM và BVDLCN tại Khoản 5 Mục I Chương này. Nội dung kiểm tra bao

gồm việc chấp hành quy chế quản trị, tiêu chuẩn kết nối, yêu cầu dữ liệu, yêu cầu tích hợp, yêu cầu an toàn, an ninh, bảo vệ dữ liệu và phạm vi sử dụng đã được phê duyệt.

Bảo đảm theo dõi nhật ký vận hành, nhật ký giao dịch, nhật ký truy cập, dấu hiệu bất thường, sai lệch dữ liệu, sai lệch trạng thái giữa các hệ thống và các vấn đề phát sinh trong quá trình khai thác. Kết quả giám sát và đánh giá là căn cứ để cho phép tiếp tục vận hành, điều chỉnh kết nối, mở rộng phạm vi ứng dụng hoặc áp dụng biện pháp kiểm soát bổ sung đối với từng hệ thống, từng ứng dụng và từng tổ chức tham gia.

Trường hợp hệ thống, ứng dụng hoặc tổ chức tham gia không còn đáp ứng yêu cầu về dữ liệu, tích hợp, an toàn, an ninh hoặc tuân thủ, cơ quan có thẩm quyền xem xét áp dụng các biện pháp xử lý phù hợp như yêu cầu khắc phục, giới hạn phạm vi khai thác, tạm dừng kết nối, thu hồi quyền truy cập hoặc tạm dừng vận hành cho đến khi đáp ứng lại đầy đủ điều kiện theo quy định. Việc kiểm soát được thực hiện thường xuyên, liên tục và gắn với trách nhiệm cụ thể của từng chủ thể tham gia.

Các vòng kiểm tra trước vận hành, cơ chế kiểm toán đối với mã nguồn smart contract và các quy định kỹ thuật về kiểm tra tuân thủ đối với DNC-Chain được thuyết minh chi tiết tại Phần A Phụ lục I kèm theo Đề án.

V. PHÁT TRIỂN NGUỒN NHÂN LỰC VÀ HỆ SINH THÁI

1. Đào tạo, bồi dưỡng nguồn nhân lực blockchain

Tổ chức đào tạo, bồi dưỡng đội ngũ nhân lực phục vụ quản trị, vận hành, tích hợp, kiểm thử, giám sát an toàn và phát triển ứng dụng trên DNC-Chain và các ứng dụng thành phần, hướng tới chỉ tiêu về nguồn nhân lực đã xác định tại tiểu mục (đ) Khoản 2 Mục III Chương III.

Chương trình đào tạo, bồi dưỡng được xây dựng theo vai trò, gắn với yêu cầu triển khai thực tế của DNC-Chain và các sản phẩm thành phần, bao gồm: Đào tạo chuyên sâu về thiết kế kiến trúc blockchain, hạ tầng và nền tảng blockchain; Đào tạo tích hợp ứng dụng và phát triển smart contract; Đào tạo chuyên sâu về quản trị khoá mật mã và kiểm toán bảo mật smart contract; Đào tạo bảo đảm an toàn, an ninh và bảo vệ dữ liệu; Đào tạo quản trị, đánh giá rủi ro và giám sát tuân thủ; Bồi dưỡng nhận thức về blockchain cho cán bộ lãnh đạo, quản lý và cán bộ chuyên môn tại các sở, ban, ngành, địa phương.

Tổ chức các mô hình thí điểm quy mô nhỏ phục vụ đào tạo thực hành, ghi nhận quy trình vận hành, xây dựng tài liệu đào tạo và kiểm chứng các quy trình kỹ thuật trước khi triển khai chính thức. Các mô hình thí điểm được tổ chức có kiểm soát, có báo cáo, có đánh giá và có cơ chế chuyển kết quả vào quy trình quản trị chung của DNC-Chain.

Tổ chức hợp tác với các cơ sở giáo dục đại học, cao đẳng, cơ sở giáo dục nghề nghiệp, viện nghiên cứu trên địa bàn thành phố và các cơ sở đào tạo có uy tín trong nước, quốc tế để phát triển các chương trình đào tạo chuyên sâu, các khóa đào tạo ngắn hạn và các chương trình thực tập, thực hành trên hạ tầng DNC-Chain; mời chuyên gia giỏi trong nước, chuyên gia người Việt Nam ở nước ngoài và chuyên gia quốc tế tham gia giảng dạy thực hành, hướng dẫn thực tập và cố vấn kỹ thuật.

Tận dụng các chương trình, nguồn lực đào tạo và phát triển nguồn nhân lực do Bộ Khoa học và Công nghệ tổ chức theo Quyết định số 2815/QĐ-TTg, bao gồm các nội dung đào tạo liên quan đến hạ tầng mạng blockchain và các lớp ứng dụng truy xuất nguồn gốc, TSMH, để cử nhân lực của thành phố tham gia; phối hợp với các viện nghiên cứu, cơ sở đào tạo được Chương trình công nghệ chiến lược quốc gia hỗ trợ để tiếp nhận, chuyển giao kiến thức, phương pháp đào tạo và kết quả nghiên cứu phục vụ triển khai Đề án.

2. Ban hành và tổ chức áp dụng Khung năng lực vận hành hệ thống blockchain thành phố

Ban hành Khung năng lực vận hành hệ thống blockchain thành phố làm căn cứ đào tạo, tuyển dụng, đánh giá và bố trí nhân lực bảo đảm vận hành DNC-Chain và các ứng dụng thành phần. Khung năng lực xác định rõ các nhóm vai trò gồm nhân lực quản trị nhà nước; nhân lực vận hành hạ tầng; nhân lực tích hợp ứng dụng; nhân lực kiểm thử, ATTT và dữ liệu; nhân lực đào tạo, nghiên cứu, chuyển giao; và nhân lực doanh nghiệp tham gia hệ sinh thái.

Tổ chức áp dụng Khung năng lực trong tuyển dụng, đào tạo, bồi dưỡng, đánh giá và bố trí nhân lực của thành phố; khuyến khích doanh nghiệp, viện nghiên cứu, cơ sở đào tạo tham gia hệ sinh thái áp dụng Khung năng lực trong hoạt động nhân sự của đơn vị. Khung năng lực được rà soát, cập nhật định kỳ theo tiến trình triển khai Đề án và lộ trình hoàn thiện tiêu chuẩn, quy chuẩn kỹ thuật quốc gia; là căn cứ để Sở Khoa học và Công nghệ phối hợp với Sở Nội vụ, các cơ sở đào tạo tổ chức các chương trình đào tạo, bồi dưỡng và phát triển nguồn nhân lực theo Khoản 1 Mục này.

3. Phát triển hệ sinh thái doanh nghiệp, viện nghiên cứu và cơ sở đào tạo

Phát triển hệ sinh thái blockchain của thành phố theo mô hình bốn nhóm:

a) Doanh nghiệp trọng tâm: gồm các doanh nghiệp công nghệ có sản phẩm, dịch vụ blockchain đã được triển khai thực tế và có năng lực cung cấp giải pháp cho Đề án theo cơ chế tham gia mở, cạnh tranh, công khai theo quy định pháp luật. Việc xác định, công nhận và làm việc với doanh nghiệp trọng tâm thực hiện theo Kế hoạch của Ủy ban nhân dân thành phố và quy định pháp luật về đấu thầu, đầu tư công, mua sắm công. Các doanh nghiệp trọng tâm tham gia hoạt động chuyển giao công nghệ, đào tạo nhân lực, hợp tác nghiên cứu phát triển và hỗ trợ triển khai các sản phẩm của Đề án theo cơ chế và phạm vi được phê duyệt.

b) Đối tác chiến lược: gồm các doanh nghiệp, tổ chức, viện nghiên cứu, trường đại học trong nước và quốc tế tham gia hợp tác chiến lược với thành phố trong phát triển DNC-Chain, chuyển giao công nghệ, phát triển nguồn nhân lực và triển khai các ứng dụng thuộc Đề án.

c) Doanh nghiệp khảo sát: phần đầu đến năm 2030 có 30 doanh nghiệp tham gia phát triển, cung cấp giải pháp, sản phẩm hoặc dịch vụ liên quan đến blockchain trên địa bàn thành phố. Doanh nghiệp được tính vào chỉ tiêu khi có tham gia trong hệ sinh thái blockchain thành phố: có hợp đồng, có sản phẩm, có kết quả nghiên cứu, có chuyển giao hoặc có đào tạo đầu ra được ghi nhận.

d) Tổ chức hỗ trợ: gồm các trường đại học, cao đẳng, viện nghiên cứu, các trung tâm đổi mới sáng tạo, các hiệp hội, tổ chức hỗ trợ khởi nghiệp, quỹ đầu tư mạo hiểm có hoạt động hỗ trợ hệ sinh thái blockchain. Tổ chức hỗ trợ đóng vai trò kết nối, đào tạo, ươm tạo và cung cấp dịch vụ tư vấn, pháp lý, tài chính cho các doanh nghiệp tham gia hệ sinh thái.

Xây dựng cơ chế làm việc định kỳ với các doanh nghiệp trọng tâm, đối tác chiến lược, doanh nghiệp khảo sát và tổ chức hỗ trợ để tháo gỡ khó khăn, chia sẻ thông tin, phối hợp triển khai các nhiệm vụ và đánh giá hiệu quả tham gia hệ sinh thái.

4. Ban hành và triển khai Kế hoạch thành phố là khách hàng đầu tiên đối với hạ tầng DNC-Chain và sản phẩm blockchain theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ

Ban hành Kế hoạch cụ thể hoá cơ chế thành phố là khách hàng đầu tiên đối với hạ tầng DNC-Chain và sản phẩm blockchain trên cơ sở Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ và hướng dẫn của Bộ Khoa học và Công nghệ. Kế hoạch xác định danh mục sản phẩm blockchain mà thành phố ưu tiên tiếp nhận; nguyên tắc ưu tiên sử dụng giải pháp do doanh nghiệp Việt Nam làm chủ công nghệ lõi khi đáp ứng yêu cầu chuyên môn, kỹ thuật, tích hợp, ATTT, ANM và phù hợp với kiến trúc DNC-Chain; hình thức gắn nhu cầu quản lý nhà nước của thành phố với việc mua sắm, thuê dịch vụ, tiếp nhận và sử dụng sản phẩm blockchain trong quy trình điều hành thực tế.

Tổ chức triển khai Kế hoạch thông qua việc gắn nhu cầu quản lý nhà nước của thành phố với mua sắm, thuê dịch vụ và tiếp nhận sản phẩm, dịch vụ blockchain do doanh nghiệp Việt Nam cung cấp; tạo thị trường ban đầu để doanh nghiệp hoàn thiện sản phẩm, đưa sản phẩm vào vận hành thực tiễn và mở rộng thương mại hoá. Việc tổ chức thực hiện bảo đảm đúng quy định của pháp luật về đấu thầu, đầu tư công, thuê dịch vụ công nghệ thông tin, quản lý và sử dụng tài sản công và các quy định chuyên ngành có liên quan; áp dụng cơ chế đặc thù của thành phố trong phạm vi cho phép; không tạo ra ưu đãi vượt thẩm quyền, không làm sai lệch nguyên tắc cạnh tranh, minh bạch và công khai.

Tổ chức các hoạt động hỗ trợ doanh nghiệp tham gia cung cấp giải pháp hạ tầng, sản phẩm, dịch vụ blockchain, đặc biệt là doanh nghiệp khởi nghiệp đổi mới sáng tạo, phù hợp với quy định pháp luật. Nội dung tập trung vào: xây dựng và tiếp cận hạ tầng DNC-Chain phục vụ phát triển, thử nghiệm sản phẩm; hỗ trợ ươm tạo, tư vấn chuyên môn, tư vấn pháp lý; hỗ trợ tham gia các chương trình xúc tiến thị trường và mở rộng khách hàng. Tổ chức các chương trình giới thiệu sản phẩm, kết nối cung-cầu, hội nghị, hội thảo chuyên đề để thúc đẩy doanh nghiệp hoàn thiện sản phẩm, tăng khả năng đáp ứng nhu cầu của thành phố và mở rộng cơ hội thương mại hoá.

5. Tổ chức đặt hàng nhiệm vụ nghiên cứu, phát triển ứng dụng blockchain cấp thành phố

Ban hành Danh mục định hướng đặt hàng nhiệm vụ nghiên cứu, phát triển ứng dụng blockchain cấp thành phố giai đoạn 2026-2030 theo quy định của Luật Khoa học, Công nghệ và Đổi mới sáng tạo số 93/2025/QH15 và Nghị định số 268/2025/NĐ-CP của Chính phủ. Danh mục xác định nội dung đặt hàng tập trung vào các hướng nghiên cứu làm chủ

công nghệ lõi gồm thiết kế kiến trúc blockchain có cấp phép, quản trị khoá mật mã và kiểm toán bảo mật smart contract; các ứng dụng thuộc danh mục sản phẩm của Đề án; các công cụ hỗ trợ tích hợp, kiểm thử, giám sát và bảo đảm an toàn; chuẩn hoá dữ liệu nguồn và xây dựng quy trình nghiệp vụ tích hợp với blockchain; đào tạo, chuyển giao công nghệ và hình thành năng lực nội sinh trong lĩnh vực blockchain.

Tổ chức triển khai các nhiệm vụ đặt hàng nghiên cứu cấp thành phố theo Danh mục đã ban hành, hướng tới chỉ tiêu tối thiểu 08 nhiệm vụ đặt hàng đến năm 2030 theo tiêu mục (đ) Khoản 2 Mục III Chương III. Đối tượng tham gia đặt hàng gồm doanh nghiệp công nghệ, viện nghiên cứu, doanh nghiệp khởi nghiệp đổi mới sáng tạo có năng lực phù hợp. Việc lựa chọn, giao nhiệm vụ, ký hợp đồng, nghiệm thu kết quả, thanh toán và quản lý sản phẩm thực hiện theo quy định pháp luật có liên quan về đầu tư công, quản lý tài chính và các quy định chuyên ngành có liên quan. Kết quả đặt hàng đạt yêu cầu được xem xét đưa vào triển khai chính thức; kết quả chưa đạt được xử lý theo quy định.

6. Phối hợp với Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai ngay

Phối hợp với Bộ Khoa học và Công nghệ trong khuôn khổ Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai ngay theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ. Nội dung phối hợp gồm:

- Đề xuất nhiệm vụ đặt hàng phát triển công nghệ lõi cho hạ tầng DNC-Chain, thành phần kỹ thuật và ứng dụng blockchain gắn với DNC-Chain;
- Kiến nghị hỗ trợ kinh phí, hỗ trợ kỹ thuật và hỗ trợ chuyển giao kết quả nghiên cứu từ Chương trình quốc gia;
- Tiếp nhận, thử nghiệm và chuyển giao áp dụng các sản phẩm, giải pháp, công nghệ lõi đầu ra của Chương trình quốc gia có liên quan đến hạ tầng mạng blockchain, TSMH trên DNC-Chain;
- Hỗ trợ doanh nghiệp, viện nghiên cứu, cơ sở đào tạo trên địa bàn tham gia mạng lưới các chủ thể được Chương trình quốc gia hỗ trợ và tham gia chuỗi cung ứng của sản phẩm công nghệ chiến lược về blockchain;
- Bảo đảm đồng bộ giữa nhiệm vụ đặt hàng cấp thành phố tại Khoản 5 Mục này và nhiệm vụ cấp quốc gia, tránh trùng lặp;
- Đẩy nhanh chuyển giao kết quả nghiên cứu, phát triển vào ứng dụng thực tiễn.

7. Hợp tác quốc tế và chuyển giao công nghệ

Tổ chức hợp tác quốc tế và chuyển giao công nghệ bảo đảm tuân thủ pháp luật Việt Nam, các cam kết quốc tế mà Việt Nam là thành viên, các yêu cầu về bảo vệ dữ liệu, ATTT, ANM và các quy định chuyên ngành có liên quan. Đặc biệt chú trọng thu hút chuyên gia người Việt Nam ở nước ngoài có kinh nghiệm nghiên cứu, phát triển và vận hành hạ tầng blockchain quy mô lớn tham gia hỗ trợ đào tạo thực hành và chuyển giao năng lực vận hành cho đội ngũ của thành phố; vận dụng các chính sách hỗ trợ phát triển nhân lực chất lượng cao đã được Hội đồng nhân dân thành phố ban hành, bao gồm Nghị

quyết số 57/2024/NQ-HĐND của Hội đồng nhân dân thành phố Đà Nẵng, khi được Hội đồng nhân dân thành phố xem xét mở rộng phạm vi áp dụng đối với lĩnh vực blockchain hoặc ban hành chính sách tương đương.

Hợp tác quốc tế được tổ chức theo hướng hỗ trợ, không thay thế định hướng làm chủ công nghệ chiến lược quốc gia đã xác định tại Khoản 5 Mục I Chương III; không tạo ra phụ thuộc một chiều vào một đối tác, một công nghệ hoặc một nền tảng bên ngoài. Kết quả hợp tác quốc tế phải hướng tới tăng cường năng lực nội sinh của thành phố và của các doanh nghiệp Việt Nam tham gia hệ sinh thái, không làm suy giảm khả năng quản trị, kiểm soát, vận hành và chủ quyền dữ liệu của thành phố đối với DNC-Chain.

Từng bước hình thành năng lực nội sinh của thành phố trong lĩnh vực blockchain thông qua chuyển giao công nghệ và chuyển giao năng lực vận hành hạ tầng từ doanh nghiệp, đối tác chiến lược trong và quốc tế, chuyên gia người Việt Nam ở nước ngoài đến đội ngũ vận hành của thành phố; xây dựng năng lực hỗ trợ kỹ thuật độc lập với tư vấn bên ngoài; hình thành đội ngũ chuyên gia có khả năng thiết kế hệ thống, phát triển thành phần, tối ưu hiệu năng, tăng cường bảo mật và tư vấn chuyên môn.

CHƯƠNG V: TỔ CHỨC THỰC HIỆN

I. TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC

Trách nhiệm tổ chức thực hiện Đề án được xác định theo chức năng, nhiệm vụ, thẩm quyền của từng cơ quan, đơn vị; cơ quan chủ trì và cơ quan phối hợp đối với từng nhiệm vụ, chương trình, dự án, sản phẩm và hạng mục đầu tư được phân công cụ thể tại Bảng 7, Bảng 8, Bảng 9 và Bảng 10 Mục III Chương IV và Phụ lục III kèm theo Đề án.

Đối với các sản phẩm ứng dụng, Đề án áp dụng thống nhất mô hình hai đầu mỗi chủ trì: cơ quan chủ trì sản phẩm chịu trách nhiệm chính về triển khai, vận hành và kết quả của sản phẩm trên hạ tầng dùng chung; cơ quan chủ trì dữ liệu nguồn, nghiệp vụ chịu trách nhiệm rà soát, chuẩn hoá, cung cấp và bảo đảm chất lượng dữ liệu nguồn phục vụ sản phẩm theo thẩm quyền quản lý ngành. Đối với các sản phẩm mà hai đầu mỗi này không trùng nhau, phân công được thể hiện rõ theo cặp chủ trì.

1. Sở Khoa học và Công nghệ

Sở Khoa học và Công nghệ là cơ quan thường trực, chủ trì điều phối tổng thể việc triển khai Đề án.

a) Tham mưu Ủy ban nhân dân thành phố ban hành kế hoạch triển khai Đề án; tổng hợp danh mục nhiệm vụ, chương trình, dự án, sản phẩm và hạng mục ưu tiên.

b) Chủ trì tổ chức xây dựng, quản trị và vận hành hạ tầng blockchain DNC-Chain; bảo đảm DNC-Chain được triển khai đồng bộ, vận hành ổn định, có khả năng tích hợp với nền tảng tích hợp, chia sẻ dữ liệu của thành phố (LGSP) và các hệ thống nguồn theo kiến trúc, tiêu chuẩn và lộ trình của Đề án.

c) Chủ trì bố trí và vận hành hạ tầng kỹ thuật nền tảng (tính toán, lưu trữ, mạng) phục vụ DNC-Chain; bảo đảm năng lực vận hành ổn định, khả năng mở rộng, sao lưu, dự phòng và khôi phục hoạt động của hạ tầng.

d) Tổ chức tích hợp kỹ thuật giữa DNC-Chain, nền tảng tích hợp, chia sẻ dữ liệu của thành phố và các hệ thống nguồn; phối hợp với Công an thành phố trong giám sát vận hành, xử lý sự cố, kiểm tra ATTT và bảo vệ dữ liệu.

đ) Chủ trì tham mưu ban hành các văn bản thể chế thực hiện Đề án. Phối hợp với Sở Tư pháp rà soát, hệ thống hóa khung pháp lý áp dụng cho Đề án; chủ động phối hợp với các đơn vị trực thuộc Bộ Khoa học và Công nghệ để bảo đảm phù hợp với Khung kiến trúc Chính phủ số và các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia.

e) Chủ trì triển khai các sản phẩm SP1, SP3, SP5 và SP6, cụ thể:

- SP1: chủ trì triển khai, phối hợp với Văn phòng Ủy ban nhân dân thành phố và các sở, ban, ngành có hệ thống nguồn trong chuẩn hoá và cung cấp dữ liệu hồ sơ điện tử;

- SP3: chủ trì triển khai, phối hợp với Sở Xây dựng và Sở Nông nghiệp và Môi trường trong xác định phạm vi dữ liệu tham chiếu và cơ chế tích hợp kỹ thuật;

- SP5: chủ trì triển khai, phối hợp với các cơ quan chủ quản dữ liệu trong chuẩn hoá, niêm yết và cấp phép khai thác dữ liệu;

- SP6: chủ trì triển khai, phối hợp với chủ sở hữu tài sản sở hữu trí tuệ và cơ quan có thẩm quyền về sở hữu trí tuệ trong chuẩn hóa dữ liệu tham chiếu và ghi nhận bằng chứng;

- SP8: chủ trì điều hành Tổ kiểm soát thử nghiệm có kiểm soát theo Quyết định số 1181/QĐ-UBND ngày 26/8/2025 của Ủy ban nhân dân thành phố; phối hợp với Sở Tài chính, Ngân hàng Nhà nước khu vực 9, Công an thành phố và Cơ quan điều hành IFC tại Đà Nẵng trong giám sát, đánh giá và xử lý vấn đề phát sinh trong phạm vi thử nghiệm.

g) Chủ trì rà soát, tổng hợp nhu cầu kinh phí thực hiện Đề án; phối hợp với Sở Tài chính xác định thứ tự ưu tiên, cơ cấu nguồn vốn, phân kỳ triển khai và phương án điều chỉnh khi cần thiết.

h) Chủ trì hướng dẫn, đôn đốc, theo dõi việc triển khai của các cơ quan chủ trì sản phẩm; tổng hợp khó khăn, vướng mắc, đề xuất phương án xử lý theo thẩm quyền hoặc báo cáo cấp có thẩm quyền.

i) Chủ trì tham mưu ban hành Khung năng lực vận hành hệ thống blockchain thành phố theo Khoản 2 Mục V Chương IV; phối hợp với Sở Nội vụ và các cơ sở đào tạo tổ chức áp dụng Khung năng lực trong đào tạo, bồi dưỡng, tuyển dụng, đánh giá và bố trí nhân lực. Chủ trì, phối hợp với các cơ quan, đơn vị, doanh nghiệp, cơ sở đào tạo và viện nghiên cứu tổ chức các chương trình đào tạo, bồi dưỡng nguồn nhân lực theo Khoản 1 Mục V Chương IV; tổ chức các hoạt động hỗ trợ doanh nghiệp, viện nghiên cứu tham gia hệ sinh thái blockchain trên địa bàn theo Khoản 3 Mục V Chương IV.

k) Chủ trì tham mưu ban hành và triển khai Kế hoạch thành phố là khách hàng đầu tiên đối với hạ tầng DNC-Chain và sản phẩm blockchain theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ và Khoản 4 Mục V Chương IV; phối hợp với Sở Tài chính, các sở, ban, ngành trong tổ chức mua sắm, thuê dịch vụ và tiếp nhận sản phẩm blockchain theo đúng quy định pháp luật về đấu thầu, đầu tư công, thuê dịch vụ công nghệ thông tin và các quy định chuyên ngành có liên quan.

l) Chủ trì tham mưu ban hành Danh mục định hướng đặt hàng nhiệm vụ nghiên cứu, phát triển ứng dụng blockchain cấp thành phố theo Khoản 5 Mục V Chương IV và Kế hoạch phối hợp với Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai ngay theo Khoản 6 Mục V Chương IV; chủ trì tổ chức triển khai các nhiệm vụ đặt hàng nghiên cứu theo quy định; phối hợp với Bộ Khoa học và Công nghệ đề xuất, đăng ký tham gia Chương trình quốc gia.

m) Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tổ chức hợp tác quốc tế, chuyển giao công nghệ và thu hút chuyên gia blockchain phục vụ triển khai Đề án theo Khoản 7 Mục V Chương IV; phối hợp với Sở Ngoại vụ, Ban Hỗ trợ và Xúc tiến đầu tư thành phố và các cơ quan liên quan trong tổ chức các hoạt động hợp tác, tiếp nhận chuyên gia, đối tác quốc tế.

n) Chủ trì tổng hợp tình hình thực hiện, kết quả triển khai, tình hình sử dụng nguồn lực, khó khăn, vướng mắc và kiến nghị; định kỳ hàng năm báo cáo Ủy ban nhân dân thành phố; phục vụ công tác sơ kết, tổng kết và đánh giá kết quả thực hiện Đề án.

o) Đề xuất tiêu chí đánh giá kết quả thực hiện Đề án của các cơ quan, đơn vị, gửi Sở Nội vụ làm căn cứ đánh giá mức độ hoàn thành nhiệm vụ hằng năm.

2. Sở Tài chính

a) Chủ trì tham mưu về cơ chế tài chính, bố trí nguồn lực ngân sách, cơ cấu nguồn vốn và lồng ghép dự toán kinh phí thực hiện Đề án, phù hợp với phân kỳ triển khai các nhiệm vụ, sản phẩm.

b) Phối hợp với Sở Khoa học và Công nghệ giám sát tài chính đối với SP8 đã được cấp Giấy chứng nhận thử nghiệm có kiểm soát theo Nghị quyết số 55/2024/NQ-HĐND ngày 13/12/2024 của Hội đồng nhân dân thành phố và Quyết định số 1181/QĐ-UBND ngày 26/8/2025 của Ủy ban nhân dân thành phố; phối hợp với Ngân hàng Nhà nước khu vực 9, Công an thành phố và Cơ quan điều hành IFC tại Đà Nẵng giám sát, đánh giá kết quả vận hành và xử lý vấn đề phát sinh trong phạm vi thử nghiệm.

c) Hướng dẫn các cơ quan, đơn vị lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện Đề án; phối hợp kiểm tra việc sử dụng kinh phí, bảo đảm đúng mục đích, tiết kiệm và hiệu quả.

d) Phối hợp với Sở Khoa học và Công nghệ rà soát nhu cầu kinh phí, cơ cấu nguồn vốn, khả năng cân đối ngân sách và phương án huy động nguồn lực ngoài ngân sách đối với các sản phẩm có yếu tố xã hội hoá, doanh nghiệp đầu tư hoặc kết hợp.

đ) Phối hợp với Sở Khoa học và Công nghệ trong triển khai Kế hoạch thành phố là khách hàng đầu tiên đối với hạ tầng DNC-Chain và sản phẩm blockchain theo Khoản 4 Mục V Chương IV; hướng dẫn quy trình mua sắm, thuê dịch vụ công nghệ thông tin và quản lý, sử dụng tài sản công đối với sản phẩm, dịch vụ blockchain do doanh nghiệp Việt Nam cung cấp, phù hợp với quy định pháp luật.

e) Phối hợp với Sở Khoa học và Công nghệ hướng dẫn tài chính, giao dự toán và hướng dẫn quyết toán đối với các nhiệm vụ đặt hàng nghiên cứu cấp thành phố về blockchain theo Khoản 5 Mục V Chương IV.

3. Văn phòng Ủy ban nhân dân thành phố

a) Phối hợp với Sở Khoa học và Công nghệ tham mưu Ủy ban nhân dân thành phố chỉ đạo, điều hành việc triển khai Đề án; theo dõi, đôn đốc các sở, ban, ngành và đơn vị liên quan thực hiện các nhiệm vụ được giao.

b) Phối hợp với Sở Khoa học và Công nghệ trong triển khai SP1; chuẩn hóa hồ sơ điện tử đi, đến, trình, duyệt tại cấp chính quyền thành phố để kết nối với DNC-Chain; phối hợp với các sở, ban, ngành trong tổ chức thực hiện.

c) Phối hợp tổng hợp thông tin, báo cáo phục vụ công tác chỉ đạo, điều hành của Ủy ban nhân dân thành phố đối với việc triển khai Đề án.

d) Phối hợp với Sở Khoa học và Công nghệ trong xây dựng, ban hành Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án theo Khoản 4 Mục I Chương IV; làm đầu mối điều phối giữa Ủy ban nhân dân thành phố và các sở, ban, ngành, đơn vị trong xử lý các vấn đề vượt thẩm quyền đơn ngành hoặc liên quan đến nhiều cơ quan.

4. Sở Giáo dục và Đào tạo

a) Chủ trì triển khai SP2; đồng thời là cơ quan chủ trì dữ liệu nguồn đối với văn bản, chứng chỉ.

b) Tổ chức lập kế hoạch thực hiện, dự toán kinh phí, triển khai, vận hành và báo cáo kết quả SP2 theo quy định.

c) Chủ trì rà soát, chuẩn hoá, hoàn thiện dữ liệu văn bản, chứng chỉ tại hệ thống nguồn của ngành giáo dục; xác định các sự kiện nghiệp vụ cần ghi nhận phục vụ xác minh, kiểm chứng và truy vết thông tin.

d) Phối hợp với Sở Khoa học và Công nghệ, các cơ sở giáo dục và doanh nghiệp cung cấp giải pháp trong quá trình tích hợp, vận hành và mở rộng ứng dụng.

đ) Phối hợp với Sở Khoa học và Công nghệ, Đại học Đà Nẵng và các cơ sở giáo dục đại học, cao đẳng, giáo dục nghề nghiệp trên địa bàn thành phố trong việc từng bước đưa nội dung blockchain vào chương trình đào tạo phù hợp với điều kiện thực tế; phối hợp triển khai các chương trình thực tập, thực hành trên hạ tầng DNC-Chain.

5. Sở Y tế

a) Chủ trì triển khai SP4; đồng thời là cơ quan chủ trì dữ liệu nguồn đối với hồ sơ y tế.

b) Tổ chức lập kế hoạch thực hiện, dự toán kinh phí, triển khai, vận hành và báo cáo kết quả SP4 theo quy định.

c) Chủ trì rà soát, chuẩn hoá, hoàn thiện dữ liệu hồ sơ y tế tại hệ thống nguồn của ngành y tế và các cơ sở khám, chữa bệnh; xác định các sự kiện nghiệp vụ cần ghi nhận phục vụ xác minh, kiểm chứng và chia sẻ thông tin theo phạm vi được phép.

d) Phối hợp với Sở Khoa học và Công nghệ, các bệnh viện, cơ sở khám, chữa bệnh và các đơn vị liên quan trong quá trình tích hợp, triển khai thí điểm, vận hành và đánh giá hiệu quả hệ thống.

6. Sở Công Thương

a) Phối hợp với Sở Khoa học và Công nghệ và các cơ quan chủ trì sản phẩm trong quá trình triển khai các sản phẩm thuộc phạm vi Đề án có liên quan đến lĩnh vực thương mại, dịch vụ thương mại điện tử, lưu thông hàng hoá và bảo vệ quyền lợi người tiêu dùng.

b) Phối hợp với Sở Văn hoá, Thể thao và Du lịch trong quá trình triển khai sản phẩm Chương trình khách hàng trung thành của thành phố (City Loyalty Program) thuộc phạm vi liên quan đến chương trình khách hàng và dịch vụ thương mại.

c) Cung cấp dữ liệu chuyên ngành thuộc lĩnh vực quản lý nhà nước về công thương khi có yêu cầu phục vụ kiểm chứng, đối soát theo quy định.

7. Sở Xây dựng

a) Là cơ quan chủ trì dữ liệu nguồn đối với hạ tầng đô thị phục vụ SP3.

b) Chủ trì rà soát, chuẩn hoá, hoàn thiện dữ liệu hạ tầng đô thị và các hệ thống thông tin chuyên ngành liên quan tại hệ thống nguồn; xác định các sự kiện nghiệp vụ cần ghi nhận phục vụ kiểm chứng, đối soát và truy vết thông tin trong quản lý, vận hành và khai thác dữ liệu đô thị.

c) Phối hợp với Sở Khoa học và Công nghệ, Sở Nông nghiệp và Môi trường, các đơn vị quản lý hạ tầng đô thị, địa phương và doanh nghiệp công nghệ trong quá trình tích hợp, triển khai thí điểm, vận hành và đánh giá kết quả SP3.

8. Sở Nông nghiệp và Môi trường

a) Là cơ quan chủ trì dữ liệu nguồn đối với môi trường và dữ liệu chuyên ngành nông nghiệp phục vụ SP3.

b) Chủ trì rà soát, chuẩn hoá, hoàn thiện dữ liệu môi trường, dữ liệu chuyên ngành nông nghiệp tại hệ thống nguồn của ngành; xác định phạm vi dữ liệu tham chiếu và các sự kiện nghiệp vụ cần ghi nhận phục vụ SP3.

c) Phối hợp với Sở Khoa học và Công nghệ và Sở Xây dựng trong việc xác định cơ chế tích hợp kỹ thuật và lộ trình triển khai SP3.

9. Sở Văn hoá, Thể thao và Du lịch

a) Chủ trì triển khai SP7; đồng thời là cơ quan chủ trì dữ liệu nguồn đối với chương trình khách hàng và dịch vụ du lịch.

b) Tổ chức lập kế hoạch thực hiện, dự toán kinh phí, triển khai, vận hành và báo cáo kết quả SP7 theo quy định.

c) Chủ trì rà soát, chuẩn hoá dữ liệu liên quan đến chương trình khách hàng, dịch vụ du lịch, văn hoá; xác định các sự kiện nghiệp vụ cần ghi nhận phục vụ quản lý, xác minh điểm thưởng, giao dịch và đối soát.

d) Phối hợp với Sở Khoa học và Công nghệ trong tích hợp, kiểm thử, vận hành sản phẩm trên DNC-Chain; phối hợp với Sở Tài chính, các doanh nghiệp du lịch, thương mại, dịch vụ và các tổ chức liên quan trong quá trình triển khai, mở rộng sản phẩm.

10. Sở Tư pháp

a) Phối hợp với Sở Khoa học và Công nghệ rà soát, hệ thống hóa khung pháp lý áp dụng cho Đề án và xây dựng danh mục văn bản cần ban hành của thành phố; tham gia rà soát, góp ý và xử lý các vấn đề pháp lý phát sinh trong quá trình thực hiện Đề án; bảo đảm các nội dung triển khai phù hợp với quy định của pháp luật và thẩm quyền của thành phố.

b) Đề xuất hoàn thiện cơ sở pháp lý, cơ chế triển khai và phương án xử lý các vướng mắc pháp lý phát sinh theo phân công hoặc theo đề nghị của cơ quan có thẩm quyền.

11. Sở Nội vụ

a) Trên cơ sở đề xuất của Sở Khoa học và Công nghệ, tham mưu bổ sung tiêu chí đánh giá kết quả thực hiện Đề án vào tiêu chí đánh giá mức độ hoàn thành nhiệm vụ hằng năm của các sở, ban, ngành và địa phương.

b) Phối hợp với Sở Khoa học và Công nghệ tham mưu bố trí đầu mối triển khai Đề án tại các cơ quan, đơn vị theo chức năng, nhiệm vụ được giao.

c) Chủ trì tham mưu về áp dụng Khung năng lực vận hành hệ thống blockchain thành phố theo Khoản 2 Mục V Chương IV trong tuyển dụng, bố trí, đánh giá cán bộ, công chức, viên chức của thành phố; phối hợp với Sở Khoa học và Công nghệ xây dựng và triển khai các chương trình đào tạo, bồi dưỡng nâng cao năng lực cho cán bộ, công chức, viên chức về blockchain, quản trị dữ liệu, ATTT và quản trị rủi ro.

d) Phối hợp tham mưu lồng ghép nội dung thi đua, khen thưởng liên quan đến triển khai Đề án trong các phong trào thi đua về khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.

12. Sở Ngoại vụ

a) Phối hợp với Sở Khoa học và Công nghệ trong tổ chức các hoạt động hợp tác quốc tế, chuyển giao công nghệ blockchain và thu hút chuyên gia quốc tế về blockchain phục vụ triển khai Đề án theo Khoản 7 Mục V Chương IV.

b) Làm đầu mối kết nối, trao đổi với các đối tác nước ngoài, tổ chức quốc tế, đại sứ quán, tổ chức phi chính phủ và các tổ chức có liên quan trong lĩnh vực blockchain, trong phạm vi chức năng, nhiệm vụ được giao.

c) Phối hợp xử lý các thủ tục ngoại giao, công hàm, thỏa thuận hợp tác và các thủ tục có yếu tố nước ngoài phục vụ chuyên gia, đoàn công tác quốc tế và các hoạt động hợp tác trong khuôn khổ Đề án.

d) Định kỳ thông báo kết quả hợp tác quốc tế về Sở Khoa học và Công nghệ để tổng hợp chung.

13. Công an thành phố Đà Nẵng

a) Phối hợp với Sở Khoa học và Công nghệ xây dựng Quy chế bảo đảm ATTT, ANM và BVDLCN đối với DNC-Chain và các ứng dụng kết nối theo Khoản 5 Mục I Chương IV; chủ trì thẩm định, kiểm tra và đánh giá ANM đối với hạ tầng DNC-Chain và các ứng dụng cốt lõi trước khi đưa vào vận hành trong phạm vi thẩm quyền cấp tỉnh; phối hợp với Bộ Công an đối với các ứng dụng thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo Luật An ninh mạng số 116/2025/QH15.

b) Chủ trì, phối hợp với Sở Khoa học và Công nghệ, Trung tâm dữ liệu thành phố bảo đảm ANM, ATTT đối với hạ tầng DNC-Chain và các ứng dụng kết nối.

c) Chủ trì kiểm tra các điều kiện ANM, ATTT, bảo vệ dữ liệu trước khi đưa vào vận hành đối với các ứng dụng có yêu cầu kiểm soát tăng cường, bao gồm các sản phẩm Tầng 4 (SP8, SP9, SP10).

d) Phối hợp rà soát, đánh giá nguy cơ, rủi ro; phát hiện dấu hiệu bất thường, lộ lọt dữ liệu hoặc dấu hiệu vi phạm pháp luật; đề xuất biện pháp phòng ngừa, cảnh báo và xử lý theo quy định.

đ) Tham gia các khóa đào tạo chuyên môn mới về kỹ thuật blockchain, truy vết và phân tích hành vi trên blockchain (on-chain), điều tra số đối với TSMH, phục vụ công tác

bảo đảm an ninh trật tự trong môi trường blockchain.

14. Cơ quan điều hành Trung tâm tài chính quốc tế Việt Nam tại Đà Nẵng

a) Là đầu mối điều phối địa phương đối với các sản phẩm thuộc Tầng 4, trọng tâm là SP9 và SP10.

b) Chủ trì phối hợp xây dựng phương án triển khai, lộ trình, yêu cầu nghiệp vụ, yêu cầu quản trị rủi ro và cơ chế phối hợp đối với SP9 và SP10 trong phạm vi cơ chế riêng của IFC Việt Nam tại Đà Nẵng theo pháp luật chuyên ngành.

c) Tổ chức theo dõi, tổng hợp, đánh giá kết quả vận hành thực tế của các mô hình thuộc Tầng 4; báo cáo theo cơ chế riêng và gửi Sở Khoa học và Công nghệ tổng hợp ở cấp Đề án; làm căn cứ để cơ quan có thẩm quyền xem xét mở rộng, điều chỉnh hoặc dừng triển khai.

d) Phối hợp với Sở Khoa học và Công nghệ, Sở Tài chính, Ngân hàng Nhà nước khu vực 9, Sở Tư pháp, Công an thành phố và các cơ quan liên quan để bảo đảm việc triển khai đúng cơ chế được cho phép, đúng phạm vi thử nghiệm, đúng yêu cầu giám sát và kiểm soát rủi ro.

đ) Rà soát điều kiện triển khai, phương án huy động nguồn lực, cơ chế phối hợp và trách nhiệm của các bên tham gia đối với các sản phẩm Tầng 4; bảo đảm ngân sách nhà nước chỉ tham gia ở phần quản lý, giám sát, tích hợp kỹ thuật, tuân thủ, quản trị rủi ro và bảo đảm chức năng quản lý nhà nước; không đầu tư phần thương mại.

15. Ngân hàng Nhà nước khu vực 9

a) Phối hợp quản lý nhà nước về tiền tệ, hoạt động ngân hàng và thanh toán đối với các sản phẩm Tầng 4 trên địa bàn trong phạm vi chức năng, nhiệm vụ được giao.

b) Phối hợp với Sở Tài chính trong giám sát và đánh giá kết quả vận hành SP8 theo cơ chế sandbox theo Nghị quyết số 55/2024/NQ-HĐND ngày 13/12/2024 của Hội đồng nhân dân thành phố và Quyết định số 1181/QĐ-UBND ngày 26/8/2025 của Ủy ban nhân dân thành phố.

c) Phối hợp với Cơ quan điều hành IFC tại Đà Nẵng, Sở Tài chính và các cơ quan liên quan đối với SP9 và SP10, bảo đảm tuân thủ pháp luật về tiền tệ, hoạt động ngân hàng, ngoại hối, chống rửa tiền và các quy định chuyên ngành có liên quan.

d) Kịp thời cảnh báo, kiến nghị biện pháp xử lý khi phát sinh rủi ro hoặc dấu hiệu bất thường liên quan đến hoạt động ngân hàng, thanh toán trong quá trình triển khai các mô hình thuộc Tầng 4.

đ) Tham gia các khóa đào tạo chuyên môn về kỹ thuật blockchain, truy vết và phân tích giao dịch trên blockchain (on-chain), nhận diện rủi ro TSMH, phục vụ công tác giám sát hoạt động ngân hàng, thanh toán và phòng, chống rửa tiền trong môi trường blockchain.

16. Các sở, ban, ngành và Ủy ban nhân dân các phường, xã, đặc khu

a) Tổ chức triển khai các nhiệm vụ của Đề án theo phân công; bố trí đầu mối phối hợp với Sở Khoa học và Công nghệ và các cơ quan chủ trì sản phẩm.

b) Rà soát, chuẩn hoá dữ liệu tại hệ thống nguồn và quy trình trao đổi dữ liệu thuộc phạm vi quản lý; bảo đảm dữ liệu nghiệp vụ tiếp tục được quản lý tại hệ thống nguồn và đáp ứng yêu cầu tích hợp, kết nối với DNC-Chain theo hướng dẫn của cơ quan có thẩm quyền.

c) Phối hợp với cơ quan chủ trì sản phẩm trong việc tổ chức tích hợp, kiểm thử, vận hành và báo cáo kết quả thực hiện đối với các sản phẩm có kết nối liên cơ quan hoặc sử dụng dữ liệu thuộc phạm vi quản lý.

d) Phối hợp với Sở Khoa học và Công nghệ, Công an thành phố trong bảo đảm ANM, ATTT, bảo vệ dữ liệu và xử lý các tình huống phát sinh.

đ) Định kỳ báo cáo kết quả thực hiện, khó khăn, vướng mắc và kiến nghị về Sở Khoa học và Công nghệ để tổng hợp.

e) Chủ trì đề xuất và triển khai các nhiệm vụ đặt hàng nghiên cứu cấp thành phố thuộc lĩnh vực quản lý của ngành theo Khoản 5 Mục V Chương IV; chủ trì xác định nhu cầu và áp dụng cơ chế thành phố là khách hàng đầu tiên đối với các sản phẩm blockchain phục vụ nhiệm vụ quản lý nhà nước của ngành theo Khoản 4 Mục V Chương IV.

17. Doanh nghiệp cung cấp công nghệ và hạ tầng kỹ thuật

a) Cung cấp các hạng mục công nghệ, nền tảng phần mềm, hạ tầng kỹ thuật và dịch vụ liên quan theo hợp đồng, thỏa thuận hoặc nhiệm vụ được giao; bảo đảm phù hợp với kiến trúc, tiêu chuẩn tích hợp, yêu cầu kỹ thuật, yêu cầu ATTT và ANM của Đề án.

b) Phối hợp với Sở Khoa học và Công nghệ và cơ quan chủ trì sản phẩm trong việc cấu hình, tích hợp, kiểm thử, vận hành, bảo trì, hỗ trợ kỹ thuật và xử lý sự cố đối với hạ tầng DNC-Chain và các ứng dụng thuộc phạm vi tham gia.

c) Bảo đảm các thành phần kỹ thuật do doanh nghiệp cung cấp đáp ứng yêu cầu về tính ổn định, khả năng mở rộng, an toàn hệ thống, bảo mật dữ liệu và khả năng kết nối; thực hiện đầy đủ trách nhiệm bảo hành, bảo trì, hỗ trợ kỹ thuật theo cam kết.

d) Chịu trách nhiệm theo hợp đồng và pháp luật về đấu thầu, giao dịch điện tử, ATTT và các quy định chuyên ngành có liên quan.

18. Doanh nghiệp, tổ chức tham gia cơ chế sandbox

a) Triển khai các giải pháp công nghệ, sản phẩm hoặc mô hình thử nghiệm đúng phạm vi, thời hạn, đối tượng, điều kiện và yêu cầu báo cáo của cơ chế sandbox đã được cơ quan có thẩm quyền phê duyệt.

b) Phối hợp với cơ quan chủ trì sản phẩm, Sở Khoa học và Công nghệ, Cơ quan điều hành IFC tại Đà Nẵng, Sở Tài chính, Ngân hàng Nhà nước khu vực 9 và các cơ quan liên quan trong cung cấp thông tin, dữ liệu, báo cáo kết quả thử nghiệm, đánh giá hiệu quả và xử lý các vấn đề phát sinh.

c) Tuân thủ kiến trúc hệ thống, tiêu chuẩn kỹ thuật, yêu cầu tích hợp với DNC-Chain và yêu cầu quản lý của thành phố.

d) Chịu trách nhiệm đối với các rủi ro phát sinh trong phạm vi hoạt động thử nghiệm theo quy định của pháp luật và nội dung cam kết; phân đầu tư thương mại do doanh nghiệp tự bảo đảm, không phát sinh nghĩa vụ ngân sách nhà nước.

19. Các cơ sở đào tạo, viện nghiên cứu

a) Phối hợp với Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan xây dựng, triển khai các chương trình đào tạo, bồi dưỡng, nghiên cứu, chuyển giao công nghệ và phát triển nguồn nhân lực phục vụ thực hiện Đề án theo Khoản 1 và Khoản 3 Mục V Chương IV.

b) Tham gia nghiên cứu, tư vấn, hỗ trợ kỹ thuật, đề xuất giải pháp công nghệ, giải pháp tích hợp, giải pháp quản trị dữ liệu, ATTT và các nội dung chuyên môn khác phục vụ triển khai Đề án theo phân công hoặc theo đề nghị của cơ quan có thẩm quyền.

c) Phối hợp tổ chức các hoạt động nghiên cứu, hội thảo khoa học, hợp tác đào tạo, hợp tác quốc tế, đổi mới sáng tạo và phát triển hệ sinh thái tri thức, công nghệ, nhân lực phục vụ triển khai blockchain trên địa bàn thành phố.

20. Các tổ chức đoàn thể và cơ quan truyền thông, báo chí

a) Phối hợp tuyên truyền, phổ biến mục tiêu, ý nghĩa, yêu cầu và lợi ích của việc triển khai Đề án; phổ biến thông tin về các kết quả triển khai, mô hình ứng dụng có hiệu quả, các hoạt động phát triển hệ sinh thái blockchain của thành phố.

b) Vận động tổ chức, cá nhân, doanh nghiệp và các chủ thể có liên quan tham gia các hoạt động ứng dụng blockchain, đổi mới sáng tạo và phát triển hệ sinh thái theo phạm vi phù hợp.

c) Tổng hợp ý kiến, kiến nghị của người dân, doanh nghiệp và các tổ chức liên quan đến việc triển khai Đề án; phản ánh đến cơ quan có thẩm quyền xem xét, xử lý theo quy định.

d) Nâng cao nhận thức của cộng đồng về yêu cầu bảo đảm an toàn, an ninh thông tin và tuân thủ pháp luật trong quá trình triển khai.

II. CƠ CHẾ PHỐI HỢP LIÊN NGÀNH VÀ XỬ LÝ VƯỚNG MẮC

1. Cơ chế phối hợp liên ngành

Sở Khoa học và Công nghệ là đầu mối điều phối chung cơ chế phối hợp liên ngành; chủ trì tổ chức họp liên ngành định kỳ hoặc đột xuất khi cần thiết; tổng hợp ý kiến và đề xuất phương án xử lý các vấn đề có liên quan đến nhiều cơ quan, đơn vị.

Đối với các nội dung có liên quan đến nhiều ngành, nhiều cấp quản lý hoặc có phạm vi tác động rộng, việc phối hợp được thực hiện theo trình tự: cơ quan đề xuất gửi nội dung phối hợp đến Sở Khoa học và Công nghệ và các cơ quan liên quan; các cơ quan liên quan có ý kiến chuyên môn theo phạm vi chức năng; Sở Khoa học và Công nghệ tổng hợp, đề xuất phương án và trình cấp có thẩm quyền xem xét thống nhất trước khi đưa vào thực hiện. Trường hợp có ý kiến khác nhau giữa các cơ quan liên quan, Sở Khoa học và Công nghệ báo cáo Ủy ban nhân dân thành phố xem xét, quyết định.

Đối với các nội dung liên quan đến ATTT, ANM, bảo vệ dữ liệu và quản trị rủi ro, cơ chế phối hợp được thực hiện với sự tham gia của Công an thành phố, Sở Khoa học và Công nghệ và các cơ quan có liên quan; kết quả phối hợp là điều kiện trước khi đưa ứng dụng vào kiểm thử và vận hành chính thức.

Đối với các sản phẩm Tầng 4, cơ chế phối hợp được thực hiện giữa Cơ quan điều hành IFC tại Đà Nẵng với Sở Tài chính, Ngân hàng Nhà nước khu vực 9, Sở Tư pháp, Công an thành phố, Sở Khoa học và Công nghệ và các cơ quan có thẩm quyền theo cơ chế riêng.

2. Xử lý vướng mắc trong quá trình thực hiện

Vướng mắc phát sinh trong quá trình triển khai Đề án được xử lý theo nguyên tắc phân cấp thẩm quyền.

a) Vướng mắc thuộc thẩm quyền của cơ quan chủ trì sản phẩm

Cơ quan chủ trì sản phẩm chủ động xử lý các vướng mắc thuộc phạm vi chức năng, nhiệm vụ của mình; báo cáo tình hình xử lý trong báo cáo định kỳ gửi Sở Khoa học và Công nghệ.

b) Vướng mắc liên ngành thuộc thẩm quyền của thành phố

Đối với các vướng mắc có liên quan đến nhiều cơ quan, đơn vị hoặc thuộc thẩm quyền giải quyết của Ủy ban nhân dân thành phố, Sở Khoa học và Công nghệ là đầu mối tổng hợp. Trình tự xử lý: cơ quan gặp vướng mắc gửi nội dung đến Sở Khoa học và Công nghệ; Sở Khoa học và Công nghệ tổ chức trao đổi với các cơ quan liên quan trong thời hạn không quá 15 ngày làm việc; tổng hợp phương án xử lý và báo cáo Ủy ban nhân dân thành phố xem xét, quyết định đối với các nội dung vượt thẩm quyền của Sở Khoa học và Công nghệ.

c) Vướng mắc vượt thẩm quyền của thành phố

Đối với các vướng mắc vượt thẩm quyền của thành phố, bao gồm các nội dung thuộc pháp luật chuyên ngành đang trong quá trình hoàn thiện, các nội dung về cơ chế liên quan đến Trung ương, các nội dung về kết nối với hệ thống do cơ quan Trung ương quản lý, các nội dung về cơ chế sandbox do cơ quan Trung ương cấp phép, Sở Khoa học và Công nghệ chủ trì tổng hợp, báo cáo Ủy ban nhân dân thành phố xem xét. Trên cơ sở ý kiến của Ủy ban nhân dân thành phố, việc báo cáo, đề xuất cơ quan có thẩm quyền ở Trung ương được thực hiện theo đúng trình tự, thủ tục quy định của pháp luật và theo chức năng, nhiệm vụ của từng cơ quan chuyên ngành có liên quan.

d) Vướng mắc đối với các sản phẩm Tầng 4

Vướng mắc phát sinh trong triển khai sản phẩm Tầng 4 xử lý theo cơ chế riêng của từng mô hình và theo pháp luật chuyên ngành. Cơ quan điều hành IFC tại Đà Nẵng, Sở Tài chính, Ngân hàng Nhà nước khu vực 9 và các cơ quan có thẩm quyền chủ trì xử lý theo phạm vi chức năng; Sở Khoa học và Công nghệ tổng hợp ở cấp Đề án, không thay thế cơ quan có thẩm quyền theo cơ chế riêng.

III. KẾ HOẠCH TRIỂN KHAI ĐỀ ÁN

Sở Khoa học và Công nghệ chủ trì, phối hợp cơ quan, đơn vị liên quan xây dựng kế hoạch triển khai Đề án trình Ủy ban nhân dân thành phố xem xét, ban hành.

Các cơ quan, đơn vị được giao chủ trì nhiệm vụ, sản phẩm có trách nhiệm xây dựng chương trình/kế hoạch chi tiết thực hiện phần công việc thuộc phạm vi phụ trách; đăng ký nhu cầu kinh phí theo quy định hiện hành, trình cấp có thẩm quyền phê duyệt để thực hiện.

IV. NGUỒN LỰC TÀI CHÍNH VÀ PHÂN BỐ NGUỒN LỰC

1. Nguyên tắc bố trí và sử dụng nguồn lực

Nguồn lực thực hiện Đề án được bố trí bám sát mục tiêu, nội dung, lộ trình và hệ thống nhiệm vụ, giải pháp đã xác định; phù hợp với pháp luật về ngân sách nhà nước, đầu tư công, khoa học và công nghệ, đấu thầu, quản lý tài sản công và các quy định pháp luật chuyên ngành có liên quan; phù hợp với khả năng cân đối ngân sách địa phương theo từng giai đoạn.

Việc bố trí nguồn lực được thực hiện có trọng tâm, trọng điểm, xuất phát từ bài toán thực tiễn và giá trị bổ sung cụ thể của từng nội dung triển khai; không đầu tư dàn trải, không triển khai theo phong trào; không bố trí kinh phí cho các nội dung chưa đáp ứng điều kiện về dữ liệu nguồn, pháp lý, tích hợp kỹ thuật hoặc tổ chức thực hiện.

Việc sử dụng nguồn lực bảo đảm đúng mục đích, đúng đối tượng, tiết kiệm, hiệu quả, công khai, minh bạch, có cơ chế kiểm tra, giám sát, hậu kiểm và đánh giá hiệu quả sử dụng. Cơ quan được giao chủ trì nhiệm vụ, sản phẩm lập dự toán chi tiết theo quy định, gửi Sở Khoa học và Công nghệ rà soát, tổng hợp trước khi trình cấp có thẩm quyền xem xét, phê duyệt.

Thứ tự ưu tiên bố trí nguồn lực được áp dụng theo trình tự:

- Các nhiệm vụ có tính nền tảng về thể chế, hạ tầng, dữ liệu, ATTT, nhân lực và các sản phẩm ứng dụng thuộc Tầng 1 được bố trí trước để tạo điều kiện triển khai toàn bộ Đề án;
- Các sản phẩm thuộc Tầng 2 và Tầng 3 được bố trí theo điều kiện chuyển mốc và kết quả đánh giá thực tiễn từng giai đoạn;
- Các sản phẩm thuộc Tầng 4 được thực hiện theo cơ chế riêng, trong đó ngân sách nhà nước chỉ tham gia ở phần quản lý, giám sát, tích hợp kỹ thuật, tuân thủ, quản trị rủi ro và bảo đảm chức năng quản lý nhà nước.

Trong quá trình thực hiện, việc điều chỉnh dự toán, cơ cấu nguồn vốn và danh mục nhiệm vụ, chương trình, dự án, sản phẩm được thực hiện theo thẩm quyền, đúng trình tự, thủ tục quy định của pháp luật, trên cơ sở kết quả đánh giá, rà soát thực tiễn của từng giai đoạn triển khai.

2. Phân định nguồn lực theo tính chất đầu tư

Nguồn lực thực hiện được phân định rõ theo chủ thể đầu tư thành ba nhóm, áp dụng thống nhất cho toàn bộ sản phẩm, hạng mục và hoạt động thuộc phạm vi Đề án.

- a) Ngân sách nhà nước do thành phố bảo đảm

Ngân sách thành phố được bố trí cho các nội dung thuộc chức năng quản lý nhà nước, gồm:

- Xây dựng thể chế, khung pháp lý, tiêu chuẩn kỹ thuật và quy chế triển khai;
- Xây dựng và vận hành hạ tầng blockchain dùng chung DNC-Chain và các mô đun nền tảng dùng chung;
- Chuẩn hóa dữ liệu, tích hợp hệ thống, bảo đảm ATTT, ANM và BVDLCN;
- Triển khai các sản phẩm phục vụ quản lý nhà nước thuộc Tầng 1 và Tầng 2;
- Quản lý nhà nước, tích hợp kỹ thuật, giám sát, tuân thủ và quản trị rủi ro đối với các sản phẩm thuộc Tầng 3 và Tầng 4;
- Đào tạo, bồi dưỡng nguồn nhân lực;
- Hỗ trợ phát triển hệ sinh thái theo các hình thức quy định của pháp luật;
- Các nhiệm vụ thuộc chức năng quản lý nhà nước khác.

Ngân sách nhà nước không được sử dụng cho phần thương mại, phần kinh doanh, phần phát hành sản phẩm tài chính, phần khai thác dịch vụ thu phí hoặc các hoạt động có bản chất đầu tư thương mại.

b) Nguồn đầu tư của doanh nghiệp

Nguồn đầu tư của doanh nghiệp là phần vốn doanh nghiệp bỏ ra để phát triển, cung cấp và vận hành phần thương mại của các sản phẩm có bản chất kinh doanh, dịch vụ thu phí hoặc hoạt động thương mại khác thuộc phạm vi Đề án. Doanh nghiệp thực hiện và tự chịu rủi ro thương mại đối với phần đầu tư này; không phát sinh cam kết ngân sách nhà nước đối với phần thương mại của doanh nghiệp.

Nguồn này được áp dụng chủ yếu đối với: phần thương mại của các sản phẩm có cơ cấu hỗn hợp thuộc Tầng 3; phần thương mại của các sản phẩm thuộc Tầng 4 thực hiện theo cơ chế sandbox hoặc cơ chế riêng gắn với IFC Việt Nam tại Đà Nẵng; một số hạng mục hạ tầng kỹ thuật do doanh nghiệp tự đầu tư theo cơ chế phù hợp với quy định của pháp luật.

Quản lý nhà nước, tích hợp kỹ thuật với DNC-Chain, giám sát, tuân thủ và bảo đảm chức năng quản lý nhà nước đối với các sản phẩm có nguồn đầu tư của doanh nghiệp do ngân sách nhà nước bảo đảm trong phạm vi được duyệt.

Việc huy động nguồn đầu tư của doanh nghiệp phải bảo đảm không làm thay đổi vai trò quản lý nhà nước của thành phố đối với nền tảng dùng chung, dữ liệu nguồn, tiêu chuẩn tích hợp, ATTT và ANM; có cơ chế kiểm tra, giám sát, hậu kiểm và trách nhiệm giải trình của doanh nghiệp tham gia.

c) Nguồn hợp pháp khác

Nguồn hợp pháp khác gồm: nguồn từ các chương trình, đề án, nhiệm vụ khoa học và công nghệ của Trung ương được phân bổ về địa phương, trong đó có Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai ngay theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng

Chính phủ; nguồn từ các chương trình hợp tác quốc tế, viện trợ, chuyển giao công nghệ; nguồn xã hội hoá, tài trợ, đặt hàng nghiên cứu của các tổ chức, cá nhân trong và ngoài nước; và các nguồn hợp pháp khác theo quy định của pháp luật.

Nguồn hợp pháp khác được tiếp nhận, quản lý và sử dụng theo quy định của pháp luật về ngân sách nhà nước, khoa học và công nghệ, đầu tư, hợp tác quốc tế và các quy định chuyên ngành có liên quan.

3. Cơ cấu phân bổ nguồn lực theo nhóm nhiệm vụ và tăng cấp độ

Trên cơ sở 05 nhóm nhiệm vụ và giải pháp, nguồn lực thực hiện Đề án được cơ cấu phân bổ như sau:

a) Nhóm nhiệm vụ về thể chế và khung pháp lý

Nguồn lực bố trí cho nhóm này phục vụ các nhiệm vụ rà soát, hệ thống hóa văn bản pháp lý; ban hành Quy chế quản trị, vận hành và khai thác DNC-Chain và Quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời ứng dụng; ban hành bộ tiêu chuẩn kỹ thuật và yêu cầu kết nối, chia sẻ, kiểm chứng dữ liệu trên DNC-Chain; ban hành Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án; ban hành Quy chế bảo đảm ATTT, ANM và BVDLCN đối với DNC-Chain và các ứng dụng kết nối.

Toàn bộ nhóm này do ngân sách thành phố bảo đảm, bố trí tập trung trong giai đoạn 2026-2027 để hoàn thiện khung thể chế trước khi mở rộng triển khai; trong giai đoạn 2028-2030, nguồn lực được tiếp tục bố trí ở mức phù hợp để rà soát, cập nhật, hoàn thiện các quy chế, quy định và tiêu chuẩn theo tiến trình hoàn thiện khung tiêu chuẩn quốc gia.

b) Nhóm nhiệm vụ về xây dựng hạ tầng DNC-Chain

Nguồn lực bố trí cho nhóm này phục vụ các nhiệm vụ chính sau:

- Tổ chức triển khai hạ tầng blockchain dùng chung của thành phố; lựa chọn và triển khai nền tảng công nghệ lõi Layer-1;

- Tổ chức mô hình kiến trúc mạng theo lộ trình 04 node trong giai đoạn 2026-2027 và mở rộng lên 06 node đến năm 2030;

- Xây dựng 07 mô đun nền tảng dùng chung của DNC-Chain, gồm: Mô đun 1 Cầu nối Đa chuỗi; Mô đun 2 Tích hợp, tạo bằng chứng xác minh và đối soát hồ sơ điện tử; Mô đun 3 Quản lý khoá và phân quyền; Mô đun 4 Quản lý giao dịch và Token; Mô đun 5 Quản lý smart contract; Mô đun 6 Quản lý ứng dụng và marketplace; Mô đun 7 Hub làm sạch dữ liệu;

- Kết nối DNC-Chain với nền tảng tích hợp, chia sẻ dữ liệu của thành phố và các hệ thống nguồn;

- Giám sát, duy trì hoạt động ổn định, dự phòng và ứng cứu sự cố.

Nhóm này kết hợp hai nguồn: ngân sách thành phố bảo đảm phần quản lý, vận hành hạ tầng lõi thuộc quyền vận hành của thành phố và các mô đun dùng chung phục vụ quản lý nhà nước; nguồn đầu tư của doanh nghiệp áp dụng đối với một số hạng mục hạ tầng kỹ thuật, mô đun có tính chất thương mại khác hoặc hạng mục do doanh nghiệp đầu tư theo

cơ chế phù hợp. Nhóm này được bố trí tập trung trong giai đoạn 2026-2027 để hình thành hạ tầng lõi phục vụ các sản phẩm ưu tiên; giai đoạn 2028-2030 tiếp tục bố trí để mở rộng, nâng cấp và hoàn thiện năng lực vận hành.

c) Nhóm nhiệm vụ về chuẩn hóa dữ liệu, tích hợp, bảo đảm ATTT, ANM

Nguồn lực bố trí cho nhóm này phục vụ chuẩn hoá dữ liệu nguồn và xác định phạm vi dữ liệu đưa vào sử dụng trên DNC-Chain; hoàn thiện cơ chế tích hợp, đối soát và kiểm chứng dữ liệu giữa DNC-Chain, nền tảng tích hợp, chia sẻ dữ liệu của thành phố và các hệ thống nguồn; bảo đảm ATTT, ANM và BVDLCN theo tiêu chuẩn, quy chuẩn kỹ thuật quốc gia; tổ chức kiểm tra, đánh giá và kiểm soát tuân thủ trong quá trình vận hành.

Toàn bộ nhóm này do ngân sách thành phố bảo đảm, được bố trí theo lộ trình gắn với nhu cầu triển khai các sản phẩm của từng tầng cấp độ. Giai đoạn 2026-2027 tập trung chuẩn hóa dữ liệu phục vụ các sản phẩm Tầng 1; giai đoạn 2028-2030 mở rộng phạm vi chuẩn hoá, tích hợp đối với các sản phẩm Tầng 2 và Tầng 3.

d) Nhóm nhiệm vụ về triển khai ứng dụng theo 04 tầng cấp độ

Đây là nhóm có quy mô nguồn lực lớn nhất của Đề án, được cơ cấu phân bổ theo từng tầng cấp độ:

Tầng 1: bố trí tập trung trong giai đoạn 2026-2027, toàn bộ từ ngân sách thành phố. Đây là nhóm ưu tiên triển khai sớm để kiểm chứng mô hình lớp tin cậy số trên hạ tầng DNC-Chain và tạo kết quả thực tiễn làm căn cứ mở rộng.

Tầng 2: bố trí trong giai đoạn 2028-2030 theo điều kiện chuyển mức quy định tại Khoản 3 Mục V Chương III, toàn bộ từ ngân sách thành phố. Việc bố trí kinh phí được thực hiện sau khi dữ liệu nguồn, yêu cầu pháp lý chuyên ngành và cơ chế phối hợp liên ngành đã được chuẩn bị đầy đủ.

Tầng 3: SP5 và SP6 do ngân sách thành phố bảo đảm phần quản lý nhà nước, tích hợp kỹ thuật với DNC-Chain và giám sát vận hành; SP7 có cơ cấu hỗn hợp, phần quản lý nhà nước, tích hợp kỹ thuật và giám sát do ngân sách thành phố bảo đảm, phần vận hành thương mại do doanh nghiệp đầu tư theo cơ chế phù hợp.

Tầng 4: thực hiện theo cơ chế riêng; phần thương mại do doanh nghiệp đầu tư theo cơ chế sandbox đã được cấp phép đối với SP8 và theo cơ chế riêng gắn với IFC Việt Nam tại Đà Nẵng đối với SP9, SP10; ngân sách thành phố chỉ tham gia ở phần quản lý, giám sát, tích hợp kỹ thuật với DNC-Chain, tuân thủ, quản trị rủi ro và bảo đảm chức năng quản lý nhà nước.

đ) Nhóm nhiệm vụ về nguồn nhân lực, năng lực triển khai và hệ sinh thái

Nguồn lực bố trí phục vụ các nhiệm vụ chính sau:

- Đào tạo, bồi dưỡng nguồn nhân lực blockchain theo Khoản 1 Mục V Chương IV;
- Ban hành và tổ chức áp dụng Khung năng lực vận hành hệ thống blockchain thành phố theo Khoản 2 Mục V Chương IV;
- Phát triển hệ sinh thái doanh nghiệp, viện nghiên cứu và cơ sở đào tạo theo Khoản 3 Mục V Chương IV;

- Ban hành và triển khai Kế hoạch thành phố là khách hàng đầu tiên đối với hạ tầng DNC-Chain và sản phẩm blockchain theo Khoản 4 Mục V Chương IV;

- Ban hành Danh mục định hướng đặt hàng nhiệm vụ nghiên cứu theo Khoản 5 Mục V Chương IV và Kế hoạch phối hợp với Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia theo Khoản 6 Mục V Chương IV; tổ chức thực hiện đặt hàng;

- Tổ chức hợp tác quốc tế và chuyển giao công nghệ theo Khoản 7 Mục V Chương IV.

Nhóm này chủ yếu do ngân sách thành phố bảo đảm; một phần có thể huy động từ nguồn hợp pháp khác, gồm nguồn từ Chương trình công nghệ chiến lược quốc gia và nguồn từ các chương trình hợp tác quốc tế theo quy định. Nguồn lực được bố trí trải đều trong giai đoạn 2026-2030, gắn với tiến độ triển khai các nhóm nhiệm vụ khác của Đề án.

Ngoài 05 nhóm nhiệm vụ nêu trên, Đề án bố trí thêm nguồn dự phòng để phục vụ các nhiệm vụ phát sinh trong quá trình triển khai. Nguồn dự phòng do ngân sách thành phố bảo đảm theo quy định của pháp luật về ngân sách nhà nước, phục vụ: các nhiệm vụ phát sinh theo yêu cầu điều chỉnh lộ trình; các nhiệm vụ phát sinh từ thay đổi pháp luật, tiêu chuẩn kỹ thuật hoặc yêu cầu quản lý chuyên ngành; các nhiệm vụ phát sinh từ kết quả đánh giá thực tiễn; và các nhiệm vụ phát sinh khác theo quyết định của cơ quan có thẩm quyền.

4. Tổng nhu cầu kinh phí thực hiện Đề án

Tổng nhu cầu kinh phí thực hiện Đề án giai đoạn 2026-2030 dự kiến là 268,0 tỷ đồng, trong đó:

Ngân sách thành phố 182,49 tỷ đồng, chiếm khoảng 68,09% tổng nhu cầu kinh phí; bố trí cho toàn bộ các nhiệm vụ thuộc chức năng quản lý nhà nước của thành phố, gồm thể chế và khung pháp lý; phân quản lý, vận hành hạ tầng DNC-Chain thuộc quyền vận hành của thành phố; dữ liệu, tích hợp, ATTT, ANM và BVDLCN; các sản phẩm ứng dụng thuộc Tầng 1 và Tầng 2; phân quản lý nhà nước và tích hợp kỹ thuật đối với các sản phẩm Tầng 3 và Tầng 4; nguồn nhân lực, năng lực triển khai và hệ sinh thái; nguồn dự phòng.

Nguồn đầu tư của doanh nghiệp và nguồn hợp pháp khác 85,51 tỷ đồng, chiếm khoảng 31,91% tổng nhu cầu kinh phí; bố trí cho một số hạng mục hạ tầng kỹ thuật do doanh nghiệp đầu tư, phần vận hành thương mại của sản phẩm có cơ cấu hỗn hợp thuộc Tầng 3 (SP6, SP7), phần thương mại của các sản phẩm thuộc Tầng 4 (SP8, SP9, SP10) thực hiện theo cơ chế riêng và một phần cho nguồn nhân lực, năng lực triển khai và hệ sinh thái từ nguồn hợp pháp khác.

Cơ cấu kinh phí chi tiết theo từng năm, từng nhóm nhiệm vụ, từng tầng cấp độ, từng sản phẩm, từng hạng mục đầu tư và từng nguồn vốn được quy định tại Phụ lục II kèm theo Đề án. Danh mục nhiệm vụ, chương trình, dự án, sản phẩm, hạng mục đầu tư và đầu mỗi chủ trì tương ứng được quy định tại Phụ lục III kèm theo Đề án. Trong quá trình triển khai, trên cơ sở kết quả đánh giá thực tiễn từng giai đoạn, Sở Khoa học và Công nghệ chủ trì phối hợp với Sở Tài chính rà soát, đề xuất cấp có thẩm quyền xem xét điều chỉnh tổng nhu cầu kinh phí, cơ cấu nguồn vốn và phân bổ giữa các nhóm nhiệm vụ, tầng

cấp độ cho phù hợp với điều kiện thực tiễn, bảo đảm đúng quy định của pháp luật và hiệu quả sử dụng nguồn lực.

CHƯƠNG VI: HIỆU QUẢ DỰ KIẾN, CHỈ TIÊU ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

I. HIỆU QUẢ DỰ KIẾN

1. Hiệu quả đối với quản lý nhà nước và dịch vụ công

Việc hình thành lớp tin cậy số dùng chung trên nền tảng DNC-Chain sẽ nâng cao độ tin cậy của dữ liệu số trong quản lý nhà nước, đồng thời tăng khả năng xác minh, kiểm chứng, truy vết và đối soát giữa các cơ quan, đơn vị trong môi trường điện tử. Các quy trình có nhiều chủ thể tham gia xử lý, có nhu cầu bảo đảm toàn vẹn hồ sơ, xác minh nguồn gốc hoặc kiểm chứng trạng thái xử lý có thêm công cụ hỗ trợ kỹ thuật độc lập.

Đối với dịch vụ công, các sản phẩm Tầng 1 trực tiếp phục vụ người dân và doanh nghiệp, trong đó Hệ thống bảo đảm toàn vẹn hồ sơ điện tử (SP1) hỗ trợ kiểm chứng trạng thái hồ sơ trong môi trường liên thông; Hệ thống xác minh văn bằng, chứng chỉ (SP2) rút ngắn thời gian xác minh và tăng độ tin cậy trong tuyển dụng, tiếp nhận hồ sơ.

Về hiệu quả tài chính, việc ứng dụng blockchain trong xác minh, đối soát và kiểm chứng rút ngắn thời gian xử lý và giảm chi phí giờ công hành chính đối với các quy trình thuộc phạm vi triển khai. Với quy mô hiện có khoảng 1.000.000 giao dịch mỗi ngày trên nền tảng tích hợp, chia sẻ dữ liệu của thành phố và khối lượng lớn hồ sơ điện tử chuyên ngành, mức tiết kiệm chi phí hành chính dự kiến đạt quy mô đáng kể; đồng thời giảm chi phí tuân thủ, đi lại và thời gian cho doanh nghiệp, người dân khi thực hiện các giao dịch cần xác minh, đối soát.

Bên cạnh đó, việc lưu vết đầy đủ các sự kiện xử lý hồ sơ và giao dịch dữ liệu trên DNC-Chain sẽ tăng khả năng hậu kiểm, kiểm tra và thanh tra; tạo căn cứ kỹ thuật độc lập phục vụ giải quyết tranh chấp và làm rõ trách nhiệm khi phát sinh sai lệch giữa các hệ thống.

2. Hiệu quả đối với hạ tầng số, dữ liệu và năng lực tích hợp

Việc xây dựng DNC-Chain với vai trò lớp tin cậy số dùng chung sẽ bổ sung một cấu phần quan trọng vào Khung kiến trúc số của thành phố, bên cạnh các nền tảng hiện có. Hạ tầng này được thiết kế theo hướng mở, có khả năng tích hợp với nền tảng tích hợp, chia sẻ dữ liệu của thành phố và các hệ thống nguồn; kết nối, liên thông với nền tảng chuỗi khối quốc gia theo tiêu chuẩn và hướng dẫn của cơ quan có thẩm quyền; liên thông với các nền tảng chuỗi khối khác có điều kiện qua Cầu nối Đa chuỗi với danh sách điểm tin cậy theo Khoản 2 Mục II Chương III.

Quá trình triển khai Đề án đồng thời thúc đẩy chuẩn hoá dữ liệu nguồn tại các hệ thống chuyên ngành theo Khung kiến trúc dữ liệu quốc gia, nâng cao chất lượng dữ liệu, mức độ liên thông và khả năng khai thác. Các cơ quan, đơn vị chủ trì dữ liệu nguồn được hỗ trợ chuẩn hóa quy trình nghiệp vụ, xác định các sự kiện cần ghi nhận và nâng cao năng lực quản trị dữ liệu của ngành.

Năng lực tích hợp liên ngành của thành phố được tăng cường thông qua việc hoàn thiện cơ chế kết nối thống nhất giữa hệ thống nguồn, nền tảng tích hợp và DNC-Chain;

cơ chế kiểm chứng độc lập giữa các cơ quan; cơ chế đối soát giữa các hệ thống chuyên ngành; làm cơ sở để thành phố từng bước mở rộng các ứng dụng có yêu cầu liên thông cao trong giai đoạn sau năm 2030.

3. Hiệu quả đối với kinh tế số, đổi mới sáng tạo và hệ sinh thái

Các sản phẩm thuộc Tầng 3 (SP5, SP6, SP7) tạo điều kiện hình thành các mô hình khai thác dữ liệu và dịch vụ số trên cơ sở dữ liệu tin cậy, hỗ trợ phát triển kinh tế dữ liệu theo định hướng tại Luật Dữ liệu số 60/2024/QH15. Việc niêm yết dữ liệu, cấp phép khai thác, xác minh giao dịch và lưu vết khai thác trên môi trường số có kiểm soát sẽ thúc đẩy kết nối cung - cầu dữ liệu, hỗ trợ phát triển dịch vụ dữ liệu, ứng dụng trí tuệ nhân tạo và các mô hình đổi mới sáng tạo trên địa bàn.

Hệ sinh thái blockchain của thành phố được phát triển có định hướng thông qua cơ chế thành phố là khách hàng đầu tiên đối với sản phẩm blockchain do doanh nghiệp Việt Nam cung cấp theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ, cơ chế đặt hàng nghiên cứu cấp thành phố và cơ chế phối hợp với Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm, dịch vụ công nghệ chiến lược ưu tiên triển khai ngay theo Quyết định số 2815/QĐ-TTg. Đến năm 2030, phần đầu có tối thiểu 30 doanh nghiệp tham gia phát triển, cung cấp giải pháp, sản phẩm hoặc dịch vụ liên quan đến blockchain trên địa bàn; hình thành mạng lưới các cơ sở đào tạo, viện nghiên cứu và tổ chức hỗ trợ cùng tham gia hệ sinh thái.

Đối với các mô hình thuộc Tầng 4, Đề án tạo khuôn khổ điều phối và giám sát ở cấp địa phương đối với các mô hình chuyên biệt gắn với IFC Việt Nam tại Đà Nẵng và cơ chế sandbox; hỗ trợ thành phố từng bước hình thành năng lực tiếp cận, giám sát và quản trị rủi ro đối với các mô hình tài chính số, TSMH trong phạm vi được pháp luật cho phép.

Đề án đồng thời đóng góp vào triển khai Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm, dịch vụ công nghệ chiến lược ưu tiên triển khai ngay tại địa phương, gắn kết quả triển khai ở Đà Nẵng với tiến trình phát triển công nghệ blockchain chung của đất nước.

4. Hiệu quả đối với năng lực tổ chức thực hiện của thành phố

Đề án chuyển cách tiếp cận blockchain từ các thử nghiệm phân tán, rời rạc sang mô hình triển khai có kiến trúc thống nhất, có lộ trình, có cơ chế quản trị và có công cụ đánh giá hiệu quả; giúp thành phố kiểm soát được phạm vi, chất lượng và rủi ro trong toàn bộ quá trình triển khai.

Việc hình thành đội ngũ nhân lực blockchain có kiến thức và kỹ năng liên quan, đạt tối thiểu 1.000 người đến năm 2030, trong đó có đội ngũ quản trị, vận hành, tích hợp, kiểm thử và giám sát an toàn, tạo năng lực nội sinh cho thành phố trong các khâu cốt lõi. Năng lực này giảm dần mức độ phụ thuộc vào nhà cung cấp bên ngoài, tăng khả năng chủ động trong vận hành và mở rộng ứng dụng.

Kinh nghiệm tổ chức triển khai DNC-Chain, các mô đun nền tảng và các sản phẩm ứng dụng sẽ hình thành năng lực tổ chức thực hiện có thể kế thừa cho các đề án, chương trình công nghệ tiếp theo của thành phố. Các cơ chế phối hợp liên ngành, chuyển mốc,

đánh giá và điều chỉnh được thiết lập trong khuôn khổ Đề án có thể tiếp tục áp dụng cho các giai đoạn sau.

5. Hiệu quả tổng thể đối với phát triển kinh tế - xã hội và đóng góp vào mục tiêu quốc gia

Đề án góp phần thực hiện mục tiêu chung tăng trưởng Tổng sản phẩm trên địa bàn (GRDP) bình quân 11%/năm giai đoạn 2026-2030 của thành phố và mục tiêu kinh tế số đạt tối thiểu 30% GDP cả nước năm 2030 theo Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị, trên 03 phương diện.

Thứ nhất, đóng góp vào tăng trưởng kinh tế số của thành phố. DNC-Chain là hạ tầng tin cậy số nền tảng cho ba lĩnh vực tạo động lực tăng trưởng chủ yếu giai đoạn 2026-2030: kinh tế dữ liệu, dịch vụ số và tài chính số. Đề án góp phần thực hiện lộ trình nâng tỷ trọng kinh tế số trong GRDP theo Kế hoạch hành động số 21-KH/TU ngày 10/9/2025 của Ban Thường vụ Thành ủy Đà Nẵng thực hiện Nghị quyết số 57-NQ/TW.

Thứ hai, đóng góp vào năng lực công nghệ chiến lược quốc gia. Đề án cụ thể hoá Chiến lược blockchain quốc gia và Danh mục công nghệ chiến lược tại địa phương; tham gia Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm, dịch vụ công nghệ chiến lược ưu tiên triển khai ngay theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ. Mục tiêu phát triển doanh nghiệp blockchain và nguồn nhân lực blockchain của thành phố đến năm 2030 đóng góp trực tiếp vào mục tiêu phát triển hệ sinh thái blockchain quốc gia.

Thứ ba, đóng góp vào cực tăng trưởng mới gắn với IFC Việt Nam tại Đà Nẵng. DNC-Chain cung cấp hạ tầng kỹ thuật dùng chung hỗ trợ giám sát, đối soát, truy vết các mô hình tài chính số chuyên biệt thuộc Tầng 4. Trong khuôn khổ cơ chế đặc thù theo Nghị quyết số 136/2024/QH15 ngày 26/6/2024 và Nghị quyết số 259/2025/QH15 ngày 11/12/2025 của Quốc hội, Đề án là cấu phần hạ tầng nền góp phần hỗ trợ thành phố hình thành năng lực giám sát, đối soát đối với các mô hình tài chính số gắn với IFC Việt Nam tại Đà Nẵng và cơ chế sandbox.

Ngoài các đóng góp trên, Đề án thúc đẩy hợp tác quốc tế trong lĩnh vực blockchain thông qua trao đổi chuyên gia, nghiên cứu, đào tạo và chuyển giao công nghệ; đồng thời nâng cao nhận thức của cán bộ, công chức, viên chức, doanh nghiệp và cộng đồng về ứng dụng blockchain.

Tổng thể, Đề án góp phần thiết thực vào định hướng phát triển Đà Nẵng trở thành trung tâm khoa học, công nghệ, đổi mới sáng tạo, tài chính và đô thị hiện đại của khu vực miền Trung theo Nghị quyết số 43-NQ/TW ngày 24/01/2019 của Bộ Chính trị.

II. HỆ THỐNG CHỈ TIÊU ĐÁNH GIÁ

1. Nguyên tắc xây dựng và áp dụng chỉ tiêu

Hệ thống chỉ tiêu bám sát mục tiêu tổng quát và các mục tiêu cụ thể đến năm 2030; không phát sinh chỉ tiêu mới ngoài phạm vi Đề án; không lặp lại các chỉ tiêu đã được xác định trong các đề án, chương trình khác của thành phố hoặc quốc gia.

Đề án không đặt chỉ tiêu cam kết tỷ trọng đóng góp trực tiếp vào GRDP của thành phố, do blockchain là công nghệ chiến lược có tính tích hợp, giá trị tạo ra phân tán trong nhiều ngành kinh tế và được lồng ghép vào chỉ tiêu chuyên ngành của các đề án, chương trình liên quan. Việc lượng hóa kết quả thực hiện Đề án thông qua hệ chỉ tiêu tổng hợp tại Khoản 2 và hệ chỉ tiêu theo sản phẩm trọng điểm tại Khoản 3 Mục này.

Mỗi chỉ tiêu xác định đầy đủ 04 thuộc tính: tên chỉ tiêu, đơn vị tính hoặc cách xác định, mốc mục tiêu theo giai đoạn, nguồn dữ liệu đo và cơ quan chịu trách nhiệm báo cáo. Chỉ tiêu không đáp ứng đủ 04 thuộc tính này không được đưa vào hệ thống.

Chỉ tiêu được phân thành 02 cấp: chỉ tiêu tổng hợp cấp Đề án phản ánh kết quả chung theo các nhóm nhiệm vụ; chỉ tiêu theo sản phẩm trọng điểm phản ánh kết quả cụ thể của từng sản phẩm ứng dụng. Đối với các sản phẩm thuộc Tầng 4, Đề án không đặt chỉ tiêu định lượng cam kết, chỉ ghi nhận tình hình triển khai và kết quả vận hành.

Chỉ tiêu được đo lường và cập nhật theo chu kỳ hằng năm, 06 tháng hoặc đột xuất khi có yêu cầu; giá trị đo được so sánh với mốc mục tiêu để xác định mức độ đạt, chưa đạt hoặc cần điều chỉnh. Kết quả đo lường chỉ tiêu là căn cứ đầu vào cho cơ chế đánh giá tại Mục III Chương này và cơ chế quản lý rủi ro, điều chỉnh Đề án tại Mục IV Chương này.

Sở Khoa học và Công nghệ chủ trì theo dõi, tổng hợp số liệu chỉ tiêu cấp Đề án; các cơ quan chủ trì sản phẩm chịu trách nhiệm cung cấp số liệu chỉ tiêu theo sản phẩm thuộc phạm vi phụ trách.

2. Hệ chỉ tiêu tổng hợp cấp Đề án

Hệ chỉ tiêu gồm 06 nhóm; trong đó 05 nhóm (I-V) bám trực tiếp 05 nhóm nhiệm vụ của Chương IV, nhóm thứ 06 phản ánh tiến độ thực hiện kinh phí theo Mục IV Chương V; toàn bộ hệ chỉ tiêu bám các mục tiêu cụ thể đến năm 2030.

Bảng 11. Hệ chỉ tiêu tổng hợp cấp Đề án đến năm 2030

TT	Nhóm chỉ tiêu và tên chỉ tiêu	Đơn vị tính	2027	2030	Nguồn dữ liệu đo / Cơ quan báo cáo
I	Nhóm chỉ tiêu về thể chế và khung pháp lý				
1	Quy chế quản trị, vận hành và khai thác DNC-Chain	Văn bản	01	01 (rà soát, cập nhật)	Sở Khoa học và Công nghệ
2	Quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời ứng dụng	Văn bản	01	01 (rà soát, cập nhật)	Sở Khoa học và Công nghệ
3	Bộ tiêu chuẩn kỹ thuật và yêu cầu kết nối DNC-Chain	Văn bản	01	01 (cập nhật định kỳ)	Sở Khoa học và Công nghệ

TT	Nhóm chỉ tiêu và tên chỉ tiêu	Đơn vị tính	2027	2030	Nguồn dữ liệu đo / Cơ quan báo cáo
4	Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án	Văn bản	01	01 (cập nhật định kỳ)	Sở Khoa học và Công nghệ, Văn phòng UBND thành phố
5	Quy chế bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân đối với DNC-Chain và các ứng dụng kết nối	Văn bản	01	01 (cập nhật định kỳ)	Sở Khoa học và Công nghệ, Công an thành phố
II	Nhóm chỉ tiêu về hạ tầng DNC-Chain				
6	Hạ tầng blockchain dùng chung DNC-Chain được đưa vào vận hành	Hạ tầng	01	01	Sở Khoa học và Công nghệ
7	Số node vận hành DNC-Chain	Node	04	06	Sở Khoa học và Công nghệ
8	Số mô đun nền tảng dùng chung của DNC-Chain được triển khai	Mô đun	07	07 (nâng cấp)	Sở Khoa học và Công nghệ
9	Tỷ lệ thời gian hoạt động ổn định của DNC-Chain	%	≥ 99,5	≥ 99,9	Sở Khoa học và Công nghệ (Trung tâm dữ liệu)
III	Nhóm chỉ tiêu về dữ liệu, tích hợp, an toàn, an ninh				
10	Số hệ thống nguồn được chuẩn hoá và kết nối với DNC-Chain qua nền tảng tích hợp, chia sẻ dữ liệu	Hệ thống	≥ 05	≥ 15	Sở Khoa học và Công nghệ, Văn phòng UBND thành phố, cơ quan, đơn vị liên quan
11	Số sự cố an toàn thông tin, an ninh mạng nghiêm trọng liên quan đến DNC-Chain không được xử lý kịp thời	Sự cố	0	0	Công an thành phố
12	Thời gian trung bình khắc phục sự cố kỹ thuật của DNC-Chain	Giờ	≤ 4	≤ 2	Sở Khoa học và Công nghệ (Trung tâm dữ liệu)

TT	Nhóm chỉ tiêu và tên chỉ tiêu	Đơn vị tính	2027	2030	Nguồn dữ liệu đo / Cơ quan báo cáo
IV	Nhóm chỉ tiêu về triển khai ứng dụng theo 04 Tầng cấp độ				
13	Số sản phẩm Tầng 1 được đưa vào vận hành chính thức	Sản phẩm	03	03 (mở rộng có điều kiện)	Sở Khoa học và Công nghệ tổng hợp
14	Số sản phẩm Tầng 2 được đưa vào vận hành chính thức	Sản phẩm	0	02	Sở Khoa học và Công nghệ tổng hợp
15	Số sản phẩm Tầng 3 được đưa vào vận hành chính thức	Sản phẩm	0	03	Sở Khoa học và Công nghệ tổng hợp
16	Số sản phẩm Tầng 4 được điều phối, tích hợp với DNC-Chain	Sản phẩm	01	03	Sở Khoa học và Công nghệ, Sở Tài chính, Cơ quan điều hành IFC tại Đà Nẵng tổng hợp
17	Tỷ lệ sản phẩm chuyển mốc đúng kế hoạch	%	≥ 80	≥ 85	Sở Khoa học và Công nghệ
V	Nhóm chỉ tiêu về nguồn nhân lực và hệ sinh thái				
18	Số nhân lực có kiến thức và kỹ năng liên quan đến blockchain trên địa bàn	Người	≥ 400	≥ 1.000	Sở Khoa học và Công nghệ, Sở Nội vụ, các cơ quan, các cơ sở đào tạo
19	Số vị trí, chức danh áp dụng Khung năng lực vận hành hệ thống blockchain thành phố	Vị trí	≥ 30	≥ 80	Sở Nội vụ, Sở Khoa học và Công nghệ
20	Số cơ sở đào tạo đưa nội dung blockchain vào chương trình đào tạo	Cơ sở	≥ 02	≥ 04	Sở Giáo dục và Đào tạo, Đại học Đà Nẵng
21	Số doanh nghiệp tham gia phát triển, cung cấp giải pháp, sản phẩm, dịch vụ liên quan đến blockchain	Doanh nghiệp	≥ 10	≥ 30	Sở Khoa học và Công nghệ

TT	Nhóm chỉ tiêu và tên chỉ tiêu	Đơn vị tính	2027	2030	Nguồn dữ liệu đo / Cơ quan báo cáo
22	Số sản phẩm blockchain do doanh nghiệp Việt Nam cung cấp được thành phố tiếp nhận theo cơ chế khách hàng đầu tiên	Sản phẩm	≥ 03	≥ 08	Sở Tài chính, Sở Khoa học và Công nghệ
23	Số nhiệm vụ đặt hàng nghiên cứu cấp thành phố về blockchain	Nhiệm vụ	≥ 03	≥ 08	Sở Khoa học và Công nghệ, các cơ quan đặt hàng
24	Số thỏa thuận, chương trình hợp tác quốc tế về blockchain đã thực hiện	Thỏa thuận / Chương trình	≥ 02	≥ 05	Sở Ngoại vụ, Sở Khoa học và Công nghệ
VI	Nhóm chỉ tiêu về thực hiện kinh phí				
25	Tỷ lệ giải ngân ngân sách thành phố bố trí cho Đề án hàng năm	%	≥ 85	≥ 90	Sở Tài chính, Sở Khoa học và Công nghệ
26	Tỷ lệ huy động nguồn đầu tư của doanh nghiệp so với kế hoạch	%	≥ 70	≥ 80	Sở Khoa học và Công nghệ

3. Hệ chỉ tiêu theo sản phẩm trọng điểm

Hệ chỉ tiêu theo sản phẩm trọng điểm phản ánh kết quả cụ thể của từng sản phẩm ứng dụng, gồm 02 loại: chỉ tiêu đầu ra (hoàn thành sản phẩm, đưa vào vận hành) và chỉ tiêu kết quả sử dụng (khối lượng xử lý, thời gian, mức độ sử dụng thực tế). Đối với sản phẩm Tầng 4, do thực hiện theo cơ chế riêng, Đề án không đặt chỉ tiêu định lượng cam kết; chỉ ghi nhận việc hoàn thành tích hợp kỹ thuật và tình hình triển khai.

Bảng 12. Hệ chỉ tiêu theo sản phẩm trọng điểm đến năm 2030

Sản phẩm	Tầng	Chỉ tiêu đầu ra	Chỉ tiêu kết quả sử dụng đến 2030	Mốc đo	Cơ quan báo cáo
SP1	1	Đưa vào vận hành trong năm 2027	Số nhóm hồ sơ điện tử được ghi nhận bằng chứng xác minh: ≥ 05 nhóm; số lượt kiểm chứng hồ sơ hàng năm: ≥ 100.000	Hàng năm	Sở Khoa học và Công nghệ

Sản phẩm	Tầng	Chỉ tiêu đầu ra	Chỉ tiêu kết quả sử dụng đến 2030	Mốc đo	Cơ quan báo cáo
SP2	1	Đưa vào vận hành trong năm 2027	Thời gian xác minh văn bằng: ≤ 01 ngày; số lượt xác minh hằng năm: ≥ 50.000	Hằng năm	Sở Giáo dục và Đào tạo
SP3	2	Đưa vào vận hành trong năm 2029	Số sự kiện vòng đời hạ tầng được ghi nhận hằng năm: ≥ 5.000 ; số khu vực thí điểm: ≥ 02	Hằng năm	Sở Khoa học và Công nghệ, Sở Xây dựng, Sở Nông nghiệp và Môi trường
SP4	2	Đưa vào vận hành trong năm 2029	Số cơ sở y tế tham gia: ≥ 05 ; số sự kiện y tế được ghi nhận hằng năm: ≥ 500.000	Hằng năm	Sở Y tế
SP5	3	Đưa vào vận hành trong năm 2029	Số bộ dữ liệu được niêm yết: ≥ 50 ; số giao dịch khai thác dữ liệu hằng năm: ≥ 1.000	Hằng năm	Sở Khoa học và Công nghệ
SP6	3	Đưa vào vận hành trong năm 2029	Số tài sản sở hữu trí tuệ được ghi nhận: ≥ 200 ; số giao dịch khai thác hằng năm: ≥ 100	Hằng năm	Sở Khoa học và Công nghệ
SP7	3	Đưa vào vận hành trong năm 2029	Số doanh nghiệp tham gia: ≥ 100 ; số giao dịch tích điểm, đổi thưởng hằng năm: ≥ 500.000	Hằng năm	Sở Văn hoá, Thể thao và Du lịch
SP8	4	Hoàn thành tích hợp lớp giám sát với DNC-Chain	Ghi nhận tình hình triển khai theo cơ chế sandbox	Theo cơ chế riêng	Sở Khoa học và Công nghệ chủ trì; Sở Tài chính phối hợp
SP9	4	Hoàn thành tích hợp lớp giám sát với DNC-Chain khi triển khai	Ghi nhận tình hình triển khai theo cơ chế riêng	Theo cơ chế riêng	Cơ quan điều hành IFC tại Đà Nẵng
SP10	4	Hoàn thành tích hợp lớp giám sát với DNC-Chain khi triển khai	Ghi nhận tình hình triển khai theo cơ chế riêng	Theo cơ chế riêng	Cơ quan điều hành IFC tại Đà Nẵng

4. Sử dụng kết quả đo lường chỉ tiêu

Kết quả đo lường chỉ tiêu là dữ liệu đầu vào cho cơ chế đánh giá tại Mục III của Chương này, cơ chế quản lý rủi ro và điều chỉnh Đề án tại Mục IV của Chương này, đồng thời là đầu vào cho chế độ báo cáo định kỳ, sơ kết, tổng kết theo Mục V Chương V.

Giá trị đo được của chỉ tiêu được so sánh với mốc mục tiêu để xác định 03 mức độ: đạt mục tiêu; chưa đạt mục tiêu nhưng trong phạm vi chấp nhận được; chưa đạt mục tiêu ở mức cần điều chỉnh. Việc xác định mức độ chấp nhận được đối với từng chỉ tiêu được quy định cụ thể tại kế hoạch triển khai hằng năm.

Đối với từng sản phẩm, kết quả đo lường chỉ tiêu đầu ra là căn cứ xem xét chuyển mốc theo lộ trình 04 mốc quy định tại Khoản 3 Mục V Chương III. Việc chuyển mốc chỉ được thực hiện khi chỉ tiêu đầu ra của mốc trước đã đạt mục tiêu.

III. CƠ CHẾ ĐÁNH GIÁ KẾT QUẢ THỰC HIỆN

1. Nguyên tắc đánh giá

Đánh giá được thực hiện khách quan, dựa trên số liệu đo lường thực tế của các chỉ tiêu tại Mục II; không đánh giá dựa trên nhận định định tính thiếu căn cứ. Các chỉ tiêu định lượng được so sánh trực tiếp với mốc mục tiêu; các chỉ tiêu định tính được đánh giá trên cơ sở bằng chứng có thể kiểm chứng.

Đánh giá được thực hiện theo đúng phạm vi Đề án. Đối với các sản phẩm thuộc Tầng 4, Đề án chỉ đánh giá tình hình triển khai và kết quả tích hợp kỹ thuật với DNC-Chain; không đánh giá nghiệp vụ chuyên ngành, không thay thế cơ quan có thẩm quyền theo cơ chế riêng.

Đánh giá được thực hiện theo 03 mức độ thống nhất: đạt mục tiêu, chưa đạt mục tiêu nhưng trong phạm vi chấp nhận được, chưa đạt mục tiêu ở mức cần điều chỉnh. Mức độ đánh giá được xác định theo giá trị đo được so với mốc mục tiêu và theo ngưỡng chấp nhận được quy định cụ thể tại kế hoạch triển khai hằng năm.

Đánh giá gắn với trách nhiệm cụ thể của từng cơ quan, đơn vị; kết quả đánh giá được sử dụng làm căn cứ đánh giá mức độ hoàn thành nhiệm vụ theo phân công, không mang tính hình thức.

Đánh giá bảo đảm tính liên tục giữa các giai đoạn: kết quả đánh giá hằng năm là đầu vào của đánh giá giữa kỳ; kết quả đánh giá giữa kỳ là đầu vào của đánh giá cuối kỳ; kết quả đánh giá cuối kỳ là căn cứ xây dựng định hướng triển khai cho giai đoạn sau năm 2030.

2. Cơ quan chủ trì và trách nhiệm phối hợp

Sở Khoa học và Công nghệ là cơ quan chủ trì tổ chức đánh giá kết quả thực hiện Đề án ở cấp thành phố, trình Ủy ban nhân dân thành phố báo cáo đánh giá.

Các cơ quan chủ trì sản phẩm có trách nhiệm cung cấp số liệu chỉ tiêu theo sản phẩm thuộc phạm vi phụ trách; giải trình nguyên nhân trong trường hợp chỉ tiêu chưa đạt mục tiêu; đề xuất biện pháp khắc phục.

Các cơ quan chủ trì dữ liệu nguồn có trách nhiệm cung cấp dữ liệu nghiệp vụ thuộc phạm vi quản lý; tham gia giải trình về chất lượng, mức độ chuẩn hoá và khả năng tích hợp của dữ liệu nguồn khi có yêu cầu.

Sở Tài chính phối hợp cung cấp số liệu về tình hình giải ngân, sử dụng kinh phí và huy động nguồn đầu tư của doanh nghiệp; tham gia đánh giá hiệu quả sử dụng nguồn lực.

Công an thành phố phối hợp cung cấp số liệu về ATTT, ANM và sự cố an ninh liên quan đến DNC-Chain; tham gia đánh giá mức độ bảo đảm ATTT, ANM trong quá trình vận hành.

Đối với các sản phẩm thuộc Tầng 4, Sở Khoa học và Công nghệ chủ trì, Sở Tài chính phối hợp đối với Sản phẩm SP8 và Cơ quan điều hành IFC tại Đà Nẵng đối với Sản phẩm SP9, SP10 là đầu mối cung cấp thông tin tình hình triển khai theo cơ chế riêng; kết quả đánh giá nghiệp vụ chuyên ngành do cơ quan có thẩm quyền theo cơ chế riêng thực hiện.

Sở Nội vụ phối hợp tiếp nhận kết quả đánh giá làm căn cứ đánh giá mức độ hoàn thành nhiệm vụ hằng năm của các cơ quan, đơn vị tham gia Đề án theo đề xuất của Sở Khoa học và Công nghệ.

3. Phương pháp đánh giá

Đánh giá được thực hiện theo phương pháp kết hợp định lượng và định tính, trong đó định lượng là chính.

Phương pháp định lượng: so sánh giá trị đo được của từng chỉ tiêu tại Mục II với mốc mục tiêu tương ứng; tính tỷ lệ đạt mục tiêu cho từng nhóm chỉ tiêu; tính tỷ lệ chuyển mốc đúng kế hoạch của các sản phẩm; tính tỷ lệ giải ngân và huy động nguồn lực.

Phương pháp định tính: phân tích nguyên nhân đối với các chỉ tiêu chưa đạt mục tiêu; đánh giá chất lượng, tính bền vững và mức độ sử dụng thực tế của các sản phẩm đã đưa vào vận hành; đánh giá mức độ tuân thủ kiến trúc, tiêu chuẩn kỹ thuật và các yêu cầu quản trị; đánh giá mức độ hài lòng của người sử dụng đối với các sản phẩm có đối tượng sử dụng là người dân, doanh nghiệp.

Kết quả đánh giá được trình bày trong báo cáo, gồm 04 nội dung chính: tổng hợp kết quả đo lường chỉ tiêu so với mục tiêu; phân tích nguyên nhân đối với các chỉ tiêu chưa đạt; nhận diện rủi ro phát sinh và đề xuất biện pháp xử lý; đề xuất điều chỉnh kế hoạch, phạm vi hoặc lộ trình khi cần thiết.

4. Thời điểm và chu kỳ đánh giá

a) Đánh giá hằng năm

Đánh giá hằng năm được thực hiện trên cơ sở số liệu chỉ tiêu của cả năm trước. Nội dung đánh giá gồm: mức độ đạt mục tiêu của từng chỉ tiêu; kết quả chuyển mốc của các sản phẩm; tình hình sử dụng nguồn lực; nhận diện rủi ro và đề xuất điều chỉnh kế hoạch năm tiếp theo. Kết quả đánh giá hằng năm là đầu vào của báo cáo năm theo Khoản 2 Mục V Chương V.

b) Đánh giá giữa kỳ năm 2028

Đánh giá giữa kỳ được thực hiện trong năm 2028, sau khi kết thúc giai đoạn 2026-2027. Nội dung đánh giá gồm: mức độ đạt mục tiêu của giai đoạn 2026-2027; kết quả triển khai các nhiệm vụ nền tảng và các sản phẩm Tầng 1; mức độ sẵn sàng chuyển sang triển khai các sản phẩm Tầng 2, Tầng 3; hiệu quả sử dụng nguồn lực; các điều chỉnh cần thiết cho giai đoạn 2028-2030. Kết quả đánh giá giữa kỳ là đầu vào của sơ kết giữa kỳ theo Tiểu mục a Khoản 3 Mục V Chương V; đồng thời là căn cứ điều chỉnh kế hoạch triển khai giai đoạn 2028-2030 khi cần thiết.

c) Đánh giá cuối kỳ năm 2030

Đánh giá cuối kỳ được thực hiện trong năm 2030, đánh giá toàn diện kết quả thực hiện Đề án giai đoạn 2026-2030. Nội dung đánh giá gồm: mức độ đạt mục tiêu tổng quát và các mục tiêu cụ thể đến năm 2030; hiệu quả đối với quản lý nhà nước, hạ tầng số, kinh tế số, hệ sinh thái và năng lực tổ chức thực hiện; hiệu quả sử dụng nguồn lực; bài học kinh nghiệm; định hướng triển khai cho giai đoạn sau năm 2030. Kết quả đánh giá cuối kỳ là đầu vào của tổng kết cuối kỳ theo Tiểu mục b Khoản 3 Mục V Chương V; là cơ sở để thành phố xây dựng định hướng tiếp tục triển khai ứng dụng blockchain trong giai đoạn sau năm 2030.

IV. QUẢN LÝ RỦI RO VÀ ĐIỀU CHỈNH ĐỀ ÁN

1. Nguyên tắc quản lý rủi ro

Rủi ro được nhận diện, phân loại, đánh giá và xử lý ngay từ giai đoạn thiết kế chính sách, không chờ đến khi phát sinh. Mỗi nhóm rủi ro được xác định rõ dấu hiệu nhận biết, ngưỡng cảnh báo, biện pháp phòng ngừa, biện pháp xử lý và cơ quan chịu trách nhiệm chủ trì.

Quản lý rủi ro gắn chặt với cơ chế đánh giá tại Mục III Chương này. Kết quả đo lường chỉ tiêu chưa đạt mục tiêu ở mức cần điều chỉnh là một trong các dấu hiệu nhận biết rủi ro; số lượng và mức độ chỉ tiêu không đạt phản ánh mức độ rủi ro tổng thể của Đề án.

Quản lý rủi ro là trách nhiệm của toàn bộ cơ quan, đơn vị tham gia Đề án, không chỉ của cơ quan điều phối. Mỗi cơ quan chủ trì sản phẩm chịu trách nhiệm quản lý rủi ro thuộc phạm vi sản phẩm; Sở Khoa học và Công nghệ chịu trách nhiệm tổng hợp, theo dõi rủi ro ở cấp Đề án và điều phối xử lý khi rủi ro vượt phạm vi một cơ quan.

Đối với các sản phẩm thuộc Tầng 4, quản lý rủi ro được thực hiện theo cơ chế riêng của từng mô hình; Đề án chỉ quản lý rủi ro về tích hợp kỹ thuật với DNC-Chain và rủi ro liên quan đến phạm vi điều phối của thành phố.

2. Các nhóm rủi ro chính và biện pháp xử lý

Các rủi ro phát sinh trong quá trình triển khai Đề án được phân thành 05 nhóm: 04 nhóm canonical theo Khoản 1 Mục II Chương III (rủi ro kỹ thuật; rủi ro tài chính và tuân thủ; rủi ro xã hội; rủi ro uy tín) và 01 nhóm rủi ro vận hành về nguồn lực và tổ chức thực hiện phục vụ giai đoạn triển khai. Với mỗi nhóm, dấu hiệu nhận biết, biện pháp phòng

ngừa, biện pháp xử lý khi phát sinh và cơ quan chủ trì được quy định thống nhất tại Bảng 13 dưới đây.

Bảng 13. Các nhóm rủi ro chính và biện pháp xử lý

Nhóm rủi ro	Dấu hiệu nhận biết	Biện pháp phòng ngừa	Biện pháp xử lý khi phát sinh	Cơ quan chủ trì
1. Rủi ro kỹ thuật (gồm hạ tầng, dữ liệu, ứng dụng)	Sự cố kỹ thuật của DNC-Chain; thời gian khắc phục vượt ngưỡng quy định; phát hiện lỗ hổng bảo mật; sự cố mất dữ liệu, lộ lọt thông tin; tấn công mạng; dữ liệu nguồn chưa chuẩn hoá hoặc không đầy đủ, không chính xác; sai lệch giữa dữ liệu trên DNC-Chain và dữ liệu tại hệ thống nguồn	Kiểm thử ATTT trước khi đưa vào vận hành; triển khai mô hình hạ tầng phân tán, dự phòng; giám sát vận hành liên tục; diễn tập ứng cứu sự cố định kỳ; rà soát, chuẩn hoá dữ liệu nguồn trước khi tích hợp; thiết lập cơ chế đối soát định kỳ giữa hệ thống nguồn và DNC-Chain	Kích hoạt quy trình ứng cứu sự cố; cô lập khu vực bị ảnh hưởng; khôi phục từ bản sao lưu; điều tra nguyên nhân; tạm dừng tích hợp đối với hệ thống có dữ liệu không đạt yêu cầu; báo cáo cấp có thẩm quyền; công bố thông tin theo quy định	Sở Khoa học và Công nghệ, Công an thành phố, các cơ quan chủ trì dữ liệu nguồn
2. Rủi ro tài chính và tuân thủ (gắn mô hình tài chính số, IFC Việt Nam tại Đà Nẵng và sandbox của thành phố)	Quy định pháp luật hoặc tiêu chuẩn kỹ thuật liên quan thay đổi; phát sinh yêu cầu pháp lý mới vượt quy định hiện hành; phát hiện nội dung triển khai chưa phù hợp với pháp luật chuyên ngành; doanh nghiệp không tham gia đủ số lượng hoặc rút khỏi cơ chế hợp tác; doanh nghiệp không tuân thủ cam kết về tích hợp kỹ thuật, tuân thủ và báo cáo; vướng mắc trong áp dụng cơ chế đặc thù về tài chính số tại Tầng 4	Rà soát pháp lý định kỳ 06 tháng một lần; cập nhật văn bản mới vào khung thể chế của Đề án; tham vấn Sở Tư pháp đối với các nội dung có yếu tố pháp lý phức tạp; xây dựng cơ chế tham gia của doanh nghiệp minh bạch, công bằng; thiết lập điều kiện và trách nhiệm của doanh nghiệp rõ ràng; áp dụng cơ chế thành phố là khách hàng đầu tiên	Tạm dừng nội dung chưa phù hợp để rà soát; điều chỉnh phạm vi, cơ chế triển khai; rà soát lại điều kiện tham gia; tìm kiếm doanh nghiệp thay thế; thu hẹp hoặc chuyển đổi cơ chế triển khai khi cần; báo cáo cấp có thẩm quyền đối với nội dung vượt thẩm quyền của thành phố	Sở Tư pháp, Sở Khoa học và Công nghệ, Sở Tài chính, Cơ quan điều hành IFC tại Đà Nẵng (đối với Tầng 4)
3. Rủi ro xã hội (bảo vệ người dùng, phòng chống lừa)	Phát sinh vụ việc lừa đảo, chiếm đoạt tài sản lợi dụng danh nghĩa Đề án hoặc DNC-Chain; phát hiện hành vi lạm dụng công nghệ	Truyền thông chính thống về mục tiêu, phạm vi và giới hạn của Đề án; công khai thông tin về các sản phẩm, doanh nghiệp	Phối hợp với cơ quan công an xử lý vi phạm; tổ chức truyền thông kịp thời để làm rõ thông tin; tạm dừng hoặc thu	Công an thành phố, Sở Khoa học và Công nghệ, các

Nhóm rủi ro	Dấu hiệu nhận biết	Biện pháp phòng ngừa	Biện pháp xử lý khi phát sinh	Cơ quan chủ trì
đảo, lạm dụng công nghệ huy động vốn trái phép)	blockchain để huy động vốn trái phép; phản ứng tiêu cực của người dân, doanh nghiệp đối với một hoặc nhiều sản phẩm	tham gia; phối hợp với cơ quan công an cảnh báo hành vi lừa đảo; áp dụng cơ chế bảo vệ người dùng theo pháp luật chuyên ngành	hẹp sản phẩm bị lạm dụng; báo cáo Ủy ban nhân dân thành phố về các tình huống nghiêm trọng	cơ quan chủ trì sản phẩm
4. Rủi ro uy tín	Thông tin sai lệch về Đề án hoặc DNC-Chain lan truyền trên mạng xã hội và phương tiện truyền thông; sự cố lớn tại một sản phẩm làm ảnh hưởng uy tín tổng thể của Đề án; phản ứng tiêu cực kéo dài của dư luận đối với một hoặc nhiều sản phẩm	Xây dựng bộ thông điệp truyền thông thống nhất; thiết lập đầu mối thông tin chính thức của Đề án; chủ động cung cấp thông tin chính xác, kịp thời cho báo chí và công luận; theo dõi dư luận và phản hồi sớm	Tổ chức truyền thông làm rõ thông tin; phối hợp với cơ quan công an xử lý thông tin sai lệch theo quy định pháp luật; báo cáo Ủy ban nhân dân thành phố về các tình huống nghiêm trọng; phối hợp với cơ quan truyền thông, báo chí trong xử lý khủng hoảng truyền thông	Sở Khoa học và Công nghệ, Công an thành phố, cơ quan truyền thông, báo chí của thành phố
5. Rủi ro về nguồn lực và tổ chức thực hiện (rủi ro vận hành cấp triển khai)	Kinh phí không được bố trí đủ theo kế hoạch; tỷ lệ giải ngân thấp; nhân lực không đủ số lượng hoặc không đủ năng lực; phối hợp liên ngành không hiệu quả; tiến độ chuyển mốc sản phẩm chậm	Lập kế hoạch triển khai hằng năm sát thực tiễn; xây dựng kế hoạch đào tạo, bồi dưỡng nhân lực có lộ trình; thiết lập cơ chế phối hợp liên ngành rõ ràng theo Mục II Chương V; theo dõi tiến độ chuyển mốc định kỳ	Điều chỉnh phạm vi, lộ trình cho phù hợp với nguồn lực thực tế; tăng cường đào tạo, bổ sung nhân lực; điều phối lại nhiệm vụ giữa các cơ quan; báo cáo Ban Chỉ đạo thực hiện Nghị quyết số 57-NQ/TW của thành phố để chỉ đạo	Sở Khoa học và Công nghệ, Sở Tài chính, Sở Nội vụ

3. Cơ chế điều chỉnh Đề án

Trong quá trình triển khai, Đề án có thể được điều chỉnh khi phát sinh các căn cứ xác đáng. Việc điều chỉnh phải bám sát mục tiêu, phạm vi, quan điểm và nguyên tắc triển khai đã xác định; không làm thay đổi nguyên tắc dữ liệu nghiệp vụ được quản lý tại hệ thống nguồn; không làm phá vỡ kiến trúc tổng thể của DNC-Chain và Khung kiến trúc số thành phố; bảo đảm phân biệt cơ chế điều chỉnh giữa các sản phẩm thuộc 04 tầng theo Mục V Chương III, không áp dụng cùng một cơ chế cho toàn bộ sản phẩm.

a) Các căn cứ xem xét điều chỉnh

Đề án được xem xét điều chỉnh khi phát sinh một hoặc nhiều trong các căn cứ:

- Thay đổi về pháp lý, tiêu chuẩn kỹ thuật hoặc yêu cầu quản lý chuyên ngành làm phát sinh yêu cầu cập nhật nội dung, phạm vi hoặc cách thức triển khai.

- Thay đổi đáng kể về công nghệ blockchain hoặc công nghệ liên quan làm phát sinh yêu cầu cập nhật kiến trúc, tiêu chuẩn kỹ thuật hoặc phương án triển khai.

- Thay đổi về điều kiện thực tiễn, bao gồm điều kiện dữ liệu nguồn, tổ chức thực hiện, nguồn lực, nhu cầu sử dụng hoặc bối cảnh phát triển của thành phố, làm phát sinh yêu cầu điều chỉnh lộ trình, phạm vi hoặc thứ tự ưu tiên.

- Kết quả đánh giá định kỳ hoặc đánh giá theo giai đoạn cho thấy cần điều chỉnh phương án triển khai, phạm vi hoặc chỉ tiêu của sản phẩm, hạng mục cụ thể.

- Kết quả quản lý rủi ro tại Khoản 2 Mục này cho thấy phát sinh rủi ro mới hoặc rủi ro vượt ngoài giả định ban đầu, làm phát sinh yêu cầu điều chỉnh biện pháp phòng ngừa, cơ chế kiểm soát hoặc phạm vi triển khai.

b) Các trường hợp xử lý sau đánh giá

Trên cơ sở kết quả đánh giá tại Mục III Chương này và kết quả quản lý rủi ro tại Khoản 2 Mục này, các tình huống xử lý được áp dụng thống nhất theo Bảng 14.

Bảng 14. Các trường hợp xử lý sau đánh giá

Tình huống	Điều kiện áp dụng	Biện pháp xử lý	Thẩm quyền quyết định
Tiếp tục triển khai theo kế hoạch	Chỉ tiêu đạt mục tiêu hoặc chưa đạt nhưng trong phạm vi chấp nhận được; không phát sinh rủi ro vượt ngưỡng	Duy trì kế hoạch hiện hành; tăng cường các biện pháp đã có	Cơ quan chủ trì sản phẩm
Điều chỉnh phạm vi sản phẩm	Chỉ tiêu kết quả sử dụng không đạt do phạm vi ban đầu không phù hợp với điều kiện thực tiễn; rủi ro dữ liệu hoặc thị trường ở mức vừa	Thu hẹp hoặc mở rộng phạm vi đối tượng áp dụng; điều chỉnh danh mục dữ liệu, nhóm hồ sơ, nhóm sản phẩm hoặc nhóm chủ thể tham gia	Sở Khoa học và Công nghệ phối hợp với cơ quan chủ trì sản phẩm, trình Ủy ban nhân dân thành phố
Điều chỉnh lộ trình triển khai	Chỉ tiêu đầu ra không đạt mốc thời gian quy định; điều kiện chuẩn bị chưa sẵn sàng; rủi ro nguồn lực hoặc tổ chức thực hiện ở mức vừa	Lùi mốc chuyển giai đoạn; kéo dài thời gian chuẩn bị; điều chỉnh lộ trình của một hoặc một số sản phẩm; điều chỉnh thứ tự ưu tiên trong kế hoạch hằng năm	Sở Khoa học và Công nghệ phối hợp với cơ quan chủ trì sản phẩm, trình Ủy ban nhân dân thành phố
Tạm dừng	Phát sinh rủi ro pháp lý, kỹ	Dừng hoạt động vận hành	Ủy ban nhân dân

Tình huống	Điều kiện áp dụng	Biện pháp xử lý	Thẩm quyền quyết định
triển khai	thuật hoặc ATTT vượt ngưỡng cho phép; điều kiện triển khai không còn phù hợp nhưng có khả năng khôi phục	trong thời gian nhất định; rà soát nguyên nhân; xây dựng phương án khắc phục; báo cáo kết quả khắc phục trước khi khôi phục	thành phố theo đề nghị của Sở Khoa học và Công nghệ; đối với Tầng 4 thực hiện theo cơ chế riêng
Chuyển đổi cơ chế triển khai	Mô hình triển khai ban đầu không còn phù hợp nhưng sản phẩm vẫn có giá trị sử dụng; cần thay đổi chủ thể đầu tư, cơ quan chủ trì hoặc cơ chế phối hợp	Điều chỉnh từ đầu tư công sang cơ chế hỗn hợp hoặc ngược lại; thay đổi cơ quan chủ trì sản phẩm hoặc cơ quan chủ trì dữ liệu nguồn; điều chỉnh cơ chế tham gia của doanh nghiệp	Ủy ban nhân dân thành phố theo đề nghị của Sở Khoa học và Công nghệ và các cơ quan liên quan
Dừng triển khai	Sản phẩm không còn khả thi về mặt pháp lý, kỹ thuật, thị trường hoặc tổ chức thực hiện; rủi ro vượt ngưỡng không có biện pháp khắc phục; hoặc mục tiêu của sản phẩm không còn phù hợp	Dừng hoàn toàn việc triển khai sản phẩm; thanh lý các hạng mục đã đầu tư theo quy định; điều chỉnh kế hoạch và dự toán; báo cáo Ban Chỉ đạo thực hiện Nghị quyết số 57-NQ/TW của thành phố	Ủy ban nhân dân thành phố theo đề nghị của Sở Khoa học và Công nghệ; đối với Tầng 4 thực hiện theo cơ chế riêng

c) Thẩm quyền và trình tự điều chỉnh

Điều chỉnh trong phạm vi kế hoạch hằng năm do Ủy ban nhân dân thành phố quyết định theo đề nghị của Sở Khoa học và Công nghệ; không làm thay đổi mục tiêu và lộ trình tổng thể của Đề án đã xác định.

Điều chỉnh về mục tiêu, phạm vi, lộ trình tổng thể hoặc cấu trúc sản phẩm của Đề án được thực hiện theo thẩm quyền, đúng trình tự, thủ tục quy định của pháp luật; trên cơ sở kết quả đánh giá giữa kỳ hoặc đánh giá cuối kỳ tại Mục III; báo cáo Ban Chỉ đạo thực hiện Nghị quyết số 57-NQ/TW của thành phố xem xét trước khi trình cấp có thẩm quyền quyết định.

Điều chỉnh đối với các sản phẩm thuộc Tầng 4 được thực hiện theo cơ chế riêng, pháp luật chuyên ngành và quyết định của cơ quan có thẩm quyền; Đề án tiếp nhận kết quả điều chỉnh ở cấp thành phố, không thay thế cơ chế riêng trong quyết định chuyên ngành.

Điều chỉnh vượt thẩm quyền của thành phố được thực hiện theo đúng trình tự, thủ tục quy định của pháp luật; Sở Khoa học và Công nghệ chủ trì tổng hợp, báo cáo Ủy ban nhân dân thành phố trước khi trình cơ quan có thẩm quyền ở Trung ương theo chức năng, nhiệm vụ của từng cơ quan chuyên ngành có liên quan.

Kết quả điều chỉnh được thông báo đến toàn bộ cơ quan, đơn vị tham gia; cập nhật vào kế hoạch triển khai hằng năm và các văn bản điều hành liên quan; công khai theo quy định của pháp luật về tiếp cận thông tin và công khai ngân sách nhà nước.

Phụ lục I

THUYẾT MINH KỸ THUẬT NỀN TẢNG DNC-CHAIN, CÁC MÔ ĐUN NỀN TẢNG DÙNG CHUNG VÀ SẢN PHẨM ỨNG DỤNG

PHẦN A: NỀN TẢNG DNC-CHAIN LAYER-1

I. ĐỊNH VỊ VÀ NGUYÊN TẮC THIẾT KẾ

1. Định vị DNC-Chain trong khung kiến trúc số thành phố

DNC-Chain là hạ tầng chuỗi khối lớp 1 có cấp phép (permissioned Layer-1) của thành phố Đà Nẵng. DNC-Chain do cơ quan chuyên trách của thành phố cấp phép, quản trị và kiểm soát trong phạm vi thẩm quyền của thành phố theo cơ chế đặc thù tại Nghị quyết số 136/2024/QH15 ngày 26/6/2024 và Nghị quyết số 259/2025/QH15 ngày 11/12/2025 của Quốc hội; đóng vai trò lớp tin cậy số trong kiến trúc số của thành phố, phục vụ xác minh, kiểm chứng, truy vết, đối soát và khai thác dữ liệu tin cậy.

DNC-Chain hình thành trên cơ sở cấu hình các giao thức Lớp nền của kiến trúc Mạng dịch vụ đa chuỗi Blockchain Việt Nam (VBSN) - hiện đang được xem xét là Nền tảng chuỗi khối quốc gia - kế thừa nguyên vẹn lớp đồng thuận, lớp xác thực, lớp quản trị khoá và lớp giám sát; đồng thời là thành phần triển khai cấp địa phương phục vụ chính quyền số, kinh tế dữ liệu, dịch vụ số và hỗ trợ Trung tâm tài chính quốc tế (IFC) Việt Nam đặt tại Đà Nẵng.

Trong kiến trúc số của thành phố, hệ thống nguồn tiếp tục quản lý dữ liệu nghiệp vụ theo chức năng, thẩm quyền; nền tảng tích hợp, chia sẻ dữ liệu của thành phố (LGSP) giữ vai trò đầu mối điều phối kết nối; lớp trung gian chuyên biệt thực hiện tích hợp kỹ thuật khi cần; DNC-Chain chỉ ghi nhận bằng chứng mật mã, dữ liệu tham chiếu và dữ liệu tối thiểu cần thiết phục vụ kiểm chứng, đối soát và truy vết.

DNC-Chain kết nối, liên thông với Nền tảng chuỗi khối quốc gia theo tiêu chuẩn và hướng dẫn của cơ quan có thẩm quyền (mặc định) và liên thông với các nền tảng chuỗi khối khác có điều kiện qua Mô đun Cầu nối Đa chuỗi (Mô đun 1) với danh sách điểm tin cậy (allowlist) do cơ quan chủ trì cấp phép. Phạm vi đối tượng liên thông bao gồm Nền tảng chuỗi khối quốc gia; các Layer-1 thuộc VBSN; các blockchain cấp phép của bộ, ngành, địa phương khác khi có nhu cầu liên thông thực tiễn; các blockchain công khai khác theo phê duyệt của cơ quan có thẩm quyền trong phạm vi hạn chế.

2. Năm nguyên tắc cơ bản của thiết kế blockchain cấp phép chủ quyền

Tham chiếu bộ nguyên tắc của các mô hình blockchain cấp phép mang tính chủ quyền quốc gia đã được chuẩn hoá (European Blockchain Services Infrastructure - EBSI của Liên minh Châu Âu, Blockchain-based Service Network - BSN của Trung Quốc) và được áp dụng tại Việt Nam thông qua VNIDChain, DNC-Chain bám sát 05 nguyên tắc cơ bản sau:

- **Tính chủ quyền (Sovereignty).** Mạng được làm chủ và kiểm soát hoàn toàn bởi các thực thể hợp pháp của Việt Nam. Cả công nghệ lõi, hạ tầng vật lý, cấu hình mạng, danh sách thành viên và khoá mật mã cốt lõi đều phải thuộc thẩm quyền quản lý của cơ quan nhà nước hoặc doanh nghiệp, tổ chức Việt Nam được phê duyệt.

- **Tính phân quyền và cấp phép (Distribution & Permission).** Mạng vận hành bởi nhiều cơ quan, không phụ thuộc một thực thể đơn lẻ; tham gia mạng, vận hành node và thay đổi cấu hình đều qua quy chế quản trị thống nhất; mô hình cấp phép (permissioned) hoặc liên minh (consortium).

- **Tính khả dụng, an toàn và bảo mật (Safety & Security).** Hệ thống vận hành liên tục, tuân thủ các tiêu chuẩn mật mã học và an toàn cấp cao; có cơ chế giám sát, dự phòng và ứng cứu sự cố.

- **Hiệu suất và khả năng mở rộng (Performance & Scalability).** Thông lượng cao, độ trễ thấp, đáp ứng ứng dụng đa ngành; có khả năng mở rộng tuyến tính khi nhu cầu sử dụng tăng.

- **Tính riêng tư theo nhu cầu (Privacy on Demand).** Hỗ trợ nhiều mức bảo mật và riêng tư dữ liệu theo yêu cầu sử dụng, tuân thủ pháp luật về bảo vệ dữ liệu cá nhân; dữ liệu cá nhân không ghi trực tiếp lên sổ cái blockchain.

3. Ba tiêu chí mở rộng và ba ràng buộc bắt buộc

Ngoài năm nguyên tắc cơ bản, DNC-Chain bám sát ba tiêu chí mở rộng: Khả năng tương tác đa chuỗi (liên thông); Tiềm năng phát triển và tích hợp (khả năng phát triển bền vững hệ sinh thái và tích hợp thuận lợi với hệ thống công nghệ hiện có); Tối ưu chi phí (chi phí triển khai và vận hành phù hợp nguồn lực cấp thành phố).

DNC-Chain đồng thời tuân thủ ba ràng buộc bắt buộc theo Đề án:

- Không triển khai các mô đun có bản chất giao dịch tài sản mã hóa công khai; không tổ chức sàn giao dịch tài sản mã hoá trên hạ tầng dùng chung. Đối với các mô hình gắn với Trung tâm tài chính quốc tế (IFC) Việt Nam đặt tại Đà Nẵng hoặc cơ chế sandbox, DNC-Chain chỉ thực hiện chức năng hỗ trợ xác minh, kiểm chứng, truy vết, đối soát và tích hợp kỹ thuật trong phạm vi được cơ quan có thẩm quyền cho phép.

- Không hình thành hạ tầng dữ liệu song song ngoài kiến trúc số hiện có của thành phố; kết nối, không thay thế LGSP và các hệ thống nguồn.

- Không ghi dữ liệu nghiệp vụ gốc và dữ liệu cá nhân lên chuỗi bất biến; chỉ ghi giá trị băm (hash), dữ liệu tham chiếu và dữ liệu tối thiểu cần thiết.

II. YÊU CẦU KỸ THUẬT

Các yêu cầu kỹ thuật của DNC-Chain dẫn xuất trực tiếp từ mục tiêu tổng quát và mục tiêu cụ thể đến năm 2030 tại Chương III Mục III và yêu cầu về hạ tầng tại Chương IV Mục II của Đề án.

Bảng A.1. Ma trận yêu cầu kỹ thuật của DNC-Chain

Yêu cầu	Chỉ tiêu định lượng / định tính	Điều khoản căn cứ tại Đề án
Phạm vi ứng dụng	Hỗ trợ đồng thời các nhóm ứng dụng chính quyền số, dịch vụ công, định danh số, quản lý hành chính, kinh tế dữ liệu trên một hạ tầng thống nhất	Chương III Mục III điểm 1, 2
Hợp đồng thông minh	Turing-complete qua EVM; tương thích hoàn toàn Solidity và hệ sinh thái Ethereum	Chương III Mục V điểm 2
Khả năng mở rộng	Mục tiêu đến 2030: 5.000 TPS trung bình, 20.000 TPS đỉnh; dự địa mở rộng 58.000 - 100.000 TPS trong các giai đoạn tiếp theo	Chương III Mục III điểm 2; Chương IV Mục II điểm 2
Cấp phép	Kiểm soát danh sách node tham gia mạng tại cả lớp đồng thuận và lớp giao tiếp (RPC)	Chương III Mục II điểm 3; Chương IV Mục II điểm 3
Tuân thủ pháp lý	Tương thích Luật Giao dịch điện tử số 20/2023/QH15, Luật Dữ liệu số 60/2024/QH15, Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, quy chuẩn mật mã dân sự của Ban Cơ yếu Chính phủ; không ghi dữ liệu cá nhân lên chuỗi bất biến	Chương III Mục II điểm 5; Chương IV Mục III
Làm chủ công nghệ	Nền tảng công nghệ lõi do doanh nghiệp, tổ chức Việt Nam làm chủ; mã nguồn có thể tùy chỉnh sâu; không phụ thuộc vào một nhà cung cấp nước ngoài đơn lẻ	Chương III Mục I điểm 5; Chương IV Mục II điểm 2
Liên thông	Liên thông mở với VBSN, các Layer-1 thuộc VBSN và các blockchain cấp phép, công khai khác được phê duyệt; mạng xác minh liên chuỗi do các cơ quan, tổ chức Việt Nam vận hành	Chương III Mục IV điểm 3; Chương IV Mục II điểm 4
Khả năng nâng cấp	Hỗ trợ nâng cấp hợp đồng thông minh và mở rộng validator không yêu cầu dừng mạng; có cơ chế đa ký và thời gian chờ (timelock) bắt buộc	Chương IV Mục II điểm 4

III. LỰA CHỌN NỀN TẢNG CÔNG NGHỆ LỖI

Việc lựa chọn nền tảng công nghệ lõi cho DNC-Chain được xem xét trên cơ sở so sánh khách quan giữa các nền tảng blockchain cấp phép chủ đạo trên thế giới theo bộ tiêu chí đã xác lập, đánh giá mức độ đáp ứng yêu cầu kỹ thuật và yêu cầu về chủ quyền công nghệ của thành phố.

1. Chín tiêu chí đánh giá

Chín tiêu chí kỹ thuật áp dụng thống nhất cho các nền tảng được so sánh:

(i) Hỗ trợ hợp đồng thông minh Turing-complete; (ii) Có cơ chế cấp phép nguyên bản hoặc bổ sung được tại lớp đồng thuận và lớp RPC; (iii) Thông lượng đã được kiểm chứng ở điều kiện sản xuất; (iv) Thời gian vận hành không sự cố của nền tảng gốc; (v) Quy mô và tính chủ động của cộng đồng phát triển; (vi) Đa dạng phần mềm máy khách (client diversity) để giảm rủi ro lỗi tập trung một client; (vii) Khả năng làm chủ công nghệ lõi và tùy chỉnh sâu; (viii) Khả năng tương thích pháp luật Việt Nam; (ix) Tham chiếu triển khai thành công trong khu vực công.

2. So sánh các nền tảng được xem xét

Bảy nền tảng blockchain cấp phép được đưa vào so sánh kỹ thuật, kết quả như sau:

Bảng A.2. So sánh các nền tảng blockchain cấp phép

Tiêu chí	Permissioned Ethereum	Hyperledger Besu	Hyperledger Fabric	FISCO BCOS	Cosmos SDK	Sonic (Fantom)	Quorum
Hợp đồng Turing-complete	Có (EVM)	Có (EVM)	Có (chaincode)	Có (EVM)	Có (CosmWasm)	Có (EVM)	Có (EVM)
Cấp phép nguyên bản	Có, hai tầng (đồng thuận + RPC)	Có (IBFT 2.0, QBFT, Clique)	Có (channel model)	Có	Tùy chỉnh qua Mô đun	Tùy chỉnh sâu	Có
TPS đã kiểm chứng	5.000 trung bình, 20.000 đỉnh; mở rộng 58.000 - 100.000	100 - 500 (IBFT); tối ưu 1.000 - 2.000	3.000 - 20.000 (lab); 500 - 3.000 (sản xuất)	2.000 - 20.000	1.000 - 10.000	2.000 - 10.000	150 - 2.000
Thời gian vận hành	Mainnet liên tục từ 30/7/2015, uptime 100%	Từ 2018	Từ 2017	Từ 2017	Từ 2019	Từ 2019	Từ 2016 (đã ngừng phát triển độc lập)
Cộng đồng phát triển	Lớn nhất thế giới	Trung bình (Linux Foundation)	Trung bình (Linux Foundation)	Chủ yếu Trung Quốc	Trung bình	Nhỏ	Đã chuyển sang Besu
Đa dạng client	7 consensus client + 9 execution client	1 client	1 client	1 client	1 client chính	1 client	1 client
Tham chiếu khu vực công quốc tế	EBSI (Liên minh Châu Âu), Bhutan (định danh)	Một số dự án doanh nghiệp	IBM Food Trust, một số dự án consortium	Chủ yếu trong khuôn khổ BSN	Chủ yếu tài chính phi tập trung	Hạn chế	-

Tiêu chí	Permissioned Ethereum	Hyperledger Besu	Hyperledger Fabric	FISCO BCOS	Cosmos SDK	Sonic (Fantom)	Quorum
	800.000 công dân), canton Zug (Thụy Sĩ)			Trung Quốc			
Tham chiếu tại Việt Nam	VNIDChain - Layer-1 tiêu chuẩn quốc gia về truy xuất nguồn gốc và định danh số, kết nối VBSN	Chưa có triển khai quy mô	Một số dự án thử nghiệm	-	-	-	-

Nguồn: Tổng hợp từ tài liệu Enterprise Ethereum Alliance, Hyperledger Foundation, tài liệu kỹ thuật chính thức của từng nền tảng, kết quả kiểm chuẩn công bố và tài liệu VNIDChain, cập nhật đến quý I/2026.

3. Phân tích ưu - nhược các phương án

Permissioned Ethereum là phương án có cộng đồng phát triển lớn nhất thế giới và là nền tảng duy nhất trong nhóm so sánh có tính đa dạng client đầy đủ (7 consensus client và 9 execution client), giúp loại trừ rủi ro lỗi phần mềm tập trung vào một client. Ethereum có tham chiếu triển khai khu vực công rộng khắp: EBSI phục vụ dịch vụ công xuyên biên giới của Liên minh Châu Âu, Bhutan đưa định danh số của 800.000 công dân lên Ethereum, canton Zug của Thụy Sĩ sử dụng cho định danh công dân. Mô hình Permissioned Ethereum giữ được ưu điểm của Ethereum mainnet đồng thời bổ sung cấp phép tại lớp đồng thuận (allowlist validator) và lớp RPC. Quan trọng hơn cho bối cảnh Việt Nam, mô hình này đã được 1Matrix triển khai thành công qua nền tảng VNIDChain - Layer-1 tiêu chuẩn quốc gia về truy xuất nguồn gốc và định danh số, kết nối với VBSN, với kết quả kiểm chuẩn đạt 5.000 TPS trung bình và 20.000 TPS đỉnh. Đây là phương án duy nhất đáp ứng đồng thời cả 09 tiêu chí.

- **Hyperledger Besu** là một client Ethereum do Linux Foundation bảo trợ, tương thích EVM hoàn toàn, có cơ chế cấp phép nguyên bản qua IBFT 2.0 và QBFT. Ưu điểm là tích hợp sẵn cấp phép phù hợp môi trường doanh nghiệp. Hạn chế căn bản là Besu là một client đơn lẻ, không tạo ra đa dạng phần mềm; thông lượng thực tế của mạng IBFT/QBFT dựa trên Besu đạt 100 - 500 TPS và tối ưu 1.000 - 2.000 TPS, thấp hơn mục tiêu 5.000 TPS của DNC-Chain. Besu phù hợp để là một trong các client trên nền tảng Permissioned Ethereum, không phù hợp làm nền tảng duy nhất.

- **Hyperledger Fabric** là nền tảng cấp phép cho consortium, thiết kế theo mô hình kênh (channel) phân vùng dữ liệu. Đạt 3.000 - 20.000 TPS trong điều kiện lab và 500 - 3.000 TPS trong triển khai sản xuất. Hạn chế lớn: Fabric không tương thích EVM, sử dụng chaincode viết bằng Go, Java hoặc Node.js. Hệ quả là toàn bộ hệ sinh thái công cụ, thư viện, chuẩn token của Ethereum không tận dụng được; đội ngũ lập trình viên Solidity

tại Việt Nam không thể áp dụng trực tiếp; các tham chiếu của EBSI, Bhutan, Thụy Sĩ và VNIDChain không áp dụng được. Mô hình channel phù hợp bài toán liên tổ chức có phân vùng rõ ràng, không phù hợp hạ tầng dùng chung đa ứng dụng như DNC-Chain.

- **FISCO BCOS** do Financial Blockchain Shenzhen Consortium (Trung Quốc) phát triển, tối ưu cho các bài toán tài chính. Thông lượng đạt 2.000 - 20.000 TPS. Hạn chế là cộng đồng phát triển chủ yếu tại Trung Quốc; tài liệu kỹ thuật phần lớn bằng tiếng Trung; các tham chiếu hầu như chỉ trong khuôn khổ BSN Trung Quốc. Việc lựa chọn FISCO BCOS sẽ đặt DNC-Chain phụ thuộc công nghệ và quy chuẩn kỹ thuật của một hệ sinh thái chủ quyền khác, không phù hợp yêu cầu độc lập công nghệ của thành phố.

- **Cosmos SDK** là framework xây dựng blockchain chuyên đề, liên thông qua giao thức IBC (Inter-Blockchain Communication), đạt 1.000 - 10.000 TPS tùy chain. Hạn chế là Cosmos không tương thích EVM nguyên bản; muốn chạy Solidity phải qua Mô đun bổ sung (Ethermint), làm tăng độ phức tạp và giảm hiệu năng. Mô hình Cosmos thiên về tạo nhiều chuỗi nhỏ chuyên biệt thay vì một hạ tầng dùng chung, trái với nguyên tắc thống nhất của DNC-Chain. Cộng đồng Cosmos chủ yếu phục vụ tài chính phi tập trung, ít tham chiếu khu vực công.

- **Sonic (tên mới của Fantom)** sử dụng đồng thuận Lachesis aBFT không đồng bộ, thông lượng 2.000 - 10.000 TPS. Hạn chế là Sonic thiết kế theo mô hình blockchain công khai, không có cơ chế cấp phép nguyên bản; muốn áp dụng cấp phép phải tùy chỉnh sâu. Phạm vi ứng dụng không bao phủ các bài toán chính quyền số, định danh công dân và quản lý hồ sơ điện tử. Cộng đồng phát triển nhỏ, ít tham chiếu khu vực công.

- **Quorum** do J.P. Morgan phát triển trên nền Go-Ethereum, đã chuyển giao cho ConsenSys và hợp nhất vào Hyperledger Besu; bản thân Quorum độc lập đã ngừng phát triển. Không còn là phương án độc lập khả dụng.

4. Kết luận lựa chọn

Trên cơ sở so sánh tại Bảng A.2 và phân tích ưu - nhược từng phương án, nền tảng công nghệ lỗi được lựa chọn cho DNC-Chain là Permissioned Ethereum (Ethereum có cấp phép), tương thích EVM hoàn toàn, với cơ chế đồng thuận Proof of Stake - Proof of Authority lai (PoS-PoA Hybrid). Quyết định lựa chọn dựa trên năm luận cứ chính:

- Là nền tảng duy nhất trong nhóm so sánh đáp ứng đồng thời cả 09 tiêu chí kỹ thuật. Ethereum mainnet vận hành liên tục trên 10 năm với uptime 100%, là minh chứng về tính bền vững; không có nền tảng trong sáu phương án còn lại đạt được thời gian vận hành tương đương.

- Là nền tảng duy nhất có đa dạng client đầy đủ (07 consensus client và 09 execution client), bảo đảm lỗi phần mềm của một client không làm gián đoạn toàn bộ mạng. Đây là yếu tố then chốt đối với hạ tầng dùng chung của cơ quan nhà nước.

- Có cộng đồng lập trình viên Solidity lớn nhất thế giới và hệ sinh thái công cụ phong phú. Đội ngũ lập trình viên Solidity tại Việt Nam có thể tham gia phát triển các ứng dụng trên DNC-Chain mà không cần đào tạo lại ngôn ngữ lập trình; các thư viện, chuẩn token (ERC-20, ERC-721, ERC-1155) và công cụ phát triển (Hardhat, Foundry, OpenZeppelin) được kế thừa nguyên bản.

- Mô hình đã được kiểm chứng tại Việt Nam thông qua VNIDChain - nền tảng Layer-1 do Công ty cổ phần 1Matrix (doanh nghiệp Việt Nam) phát triển và làm chủ công nghệ lõi. VNIDChain được định vị là blockchain tiêu chuẩn quốc gia về truy xuất nguồn gốc và định danh số, kết nối với VBSN. Kết quả kiểm chuẩn thực nghiệm của VNIDChain trên cấu hình 06 full node đạt thông lượng trung bình 5.000 TPS, đỉnh 20.000 TPS, thời gian hoàn tất khối 1,5 - 2 blocks; khả năng mở rộng lý thuyết 58.000 - 100.000 TPS. Kết quả này chứng minh mô hình Permissioned Ethereum với PoS-PoA lai đã được doanh nghiệp Việt Nam triển khai thành công ở quy mô quốc gia, đáp ứng đầy đủ yêu cầu kỹ thuật và chủ quyền công nghệ.

- Enterprise Ethereum Alliance đã phát triển Enterprise Ethereum Client Specification phiên bản 6 và Permissioned Blockchains Specification phiên bản 2 phù hợp khu vực công, là khung tham chiếu kỹ thuật chuẩn hoá đã được EBSI áp dụng tuân thủ GDPR. Điều này cho thấy khả năng tương thích cao với Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 của Việt Nam.

5. Định hướng triển khai bởi doanh nghiệp Việt Nam

Việc lựa chọn Permissioned Ethereum làm công nghệ lõi bảo đảm DNC-Chain có thể được triển khai toàn bộ trong nước bởi doanh nghiệp, tổ chức Việt Nam, tuân thủ định hướng tại Chương IV Mục II điểm 2 của Đề án, Quyết định số 1131/QĐ-TTg của Thủ tướng Chính phủ về Danh mục công nghệ chiến lược và Quyết định số 2815/QĐ-TTg về Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai nhanh.

Các cấu phần triển khai DNC-Chain (thiết kế hệ thống, phát triển hợp đồng thông minh, tùy chỉnh client, cấu hình hạ tầng, tích hợp, vận hành và bảo trì) đều có thể thực hiện bởi các doanh nghiệp công nghệ trong nước đã làm chủ mô hình Permissioned Ethereum. Trường hợp điển hình là 1Matrix đã phát triển, triển khai và vận hành VNIDChain trên mô hình này, cho thấy năng lực của doanh nghiệp Việt Nam trong việc làm chủ toàn diện công nghệ lõi, từ tùy chỉnh mã nguồn đến kiểm chuẩn hiệu năng.

DNC-Chain triển khai dưới dạng Layer-1 riêng của thành phố Đà Nẵng với tham số vận hành, danh sách validator và cơ chế quản trị trong phạm vi thẩm quyền của thành phố theo cơ chế đặc thù tại Nghị quyết số 136/2024/QH15 ngày 26/6/2024 và Nghị quyết số 259/2025/QH15 ngày 11/12/2025 của Quốc hội; kế thừa các Lớp nền của kiến trúc VBSN theo Khoản 1 Mục I của Phần A này, không phải bản sao hoặc phân nhánh của Ethereum công khai hay các Layer-1 thương mại khác. Trong quá trình lựa chọn đơn vị triển khai cụ thể, thành phố ưu tiên các doanh nghiệp Việt Nam đã có kinh nghiệm làm chủ và vận hành mô hình Permissioned Ethereum + PoS-PoA trên thực tế, bảo đảm đầy đủ năng lực kỹ thuật, an toàn, an ninh và khả năng tích hợp với kiến trúc số của thành phố.

6. Tùy chỉnh so với Ethereum công khai

DNC-Chain, theo mô hình Permissioned Ethereum, được tùy chỉnh từ Ethereum công khai (mainnet) theo bốn nhóm nội dung, thực hiện ở lớp đồng thuận và lớp truy cập dữ liệu theo mô hình đã được Enterprise Ethereum Alliance chuẩn hóa và VNIDChain triển khai thực tế:

- **Nhóm 1 - Chuyển đổi cơ chế đồng thuận.** Chuyển từ Proof of Stake không cấp phép (permissionless) sang Proof of Stake cấp phép (permissioned), kết hợp yếu tố Proof of Authority. Chỉ các validator đã được cơ quan có thẩm quyền phê duyệt (whitelisted) mới tham gia xác minh giao dịch và tạo khối. Chi tiết tại Mục V của Phần A này.

- **Nhóm 2 - Bổ sung phân quyền tại lớp RPC.** Xác minh điểm cuối bằng chữ ký số theo chuẩn ERC-191 hoặc quy chuẩn tương đương do Ban Cơ yếu Chính phủ chấp thuận. Các client không có chứng thư số hợp lệ bị chặn ngay tại lớp mạng. Chi tiết tại Mục VII.

- **Nhóm 3 - Tham số kinh tế phi thương mại.** Phí giao dịch (gas fee) đặt ở mức tối thiểu phục vụ chống tấn công từ chối dịch vụ; token nội bộ dùng làm đơn vị tính phí gas và stake của validator, không phải tài sản thương mại công khai, không giao dịch trên thị trường. Validator vận hành theo trách nhiệm công vụ hoặc theo cơ chế hợp đồng dịch vụ với cơ quan có thẩm quyền.

- **Nhóm 4 - Cơ chế nâng cấp có kiểm soát.** Hợp đồng thông minh của các mô đun nền tảng và sản phẩm ứng dụng sử dụng mô hình Proxy Upgrade Pattern (ERC-1967) kết hợp đa ký và thời gian chờ (timelock) tối thiểu 48 giờ trước khi thực thi thay đổi. Danh sách validator quản lý qua hợp đồng quản trị on-chain, cho phép thêm/thay thế/loại validator không cần dừng mạng (no hard fork required).

IV. KIẾN TRÚC HỆ THỐNG

DNC-Chain thiết kế theo cấu trúc phân lớp, kế thừa mô hình chuẩn Enterprise Ethereum Permissioned Networks theo Enterprise Ethereum Client Specification v6 của Enterprise Ethereum Alliance. Cấu trúc gồm năm lớp chính, với tính chỉnh tại lớp đồng thuận và lớp giao tiếp để bổ sung cơ chế cấp phép, phân quyền truy cập dữ liệu và tối ưu hiệu suất.

Bảng A.3. Kiến trúc năm lớp của DNC-Chain

Lớp	Thành phần	Mô tả
Lớp Ứng dụng (Application Layer)	DApps và Smart Contracts	Hợp đồng thông minh viết bằng Solidity triển khai trên EVM; DApps của 10 sản phẩm ứng dụng và 07 mô đun nền tảng
Lớp Thực thi (Execution Layer)	EVM và State	Cấu trúc cây Merkle-Patricia, quản lý trạng thái và giao dịch; tương thích hoàn toàn với Ethereum mainnet
Lớp Đồng thuận (Consensus Layer)	PoS-PoA Hybrid	Cơ chế đồng thuận lai giữa Proof of Stake và Proof of Authority, có cấp phép tại lõi đồng thuận
Lớp Mạng (Network Layer)	devp2p / libp2p	Mạng ngang hàng có kiểm soát truy cập bằng danh sách (ACL); allowlist validator và RPC node

Lớp	Thành phần	Mô tả
Lớp Dữ liệu (Data Layer)	Blocks và Database	Tùy chỉnh cơ chế phân quyền truy cập dữ liệu tại RPC; hỗ trợ bảo mật và riêng tư dữ liệu ngay tại lớp lưu trữ

Các đặc trưng kỹ thuật chính của kiến trúc DNC-Chain gồm:

Cơ chế cấp phép và phân quyền hai tầng. Áp dụng đồng thời tại lớp đồng thuận (allowlist validator) và lớp RPC (xác minh chứng thư số chứng thực điểm cuối), chỉ các node được phê duyệt mới tham gia được mạng ở cả hai lớp.

Tối ưu hiệu suất theo chuẩn Permissioned Ethereum. Mục tiêu thiết kế đạt 5.000 TPS trung bình, 20.000 TPS đỉnh, độ trễ 1 - 2 giây, dư địa mở rộng 58.000 - 100.000 TPS. Các chỉ tiêu này đã được kiểm chứng thực nghiệm trên nền tảng VNIDChain cùng mô hình, cấu hình cụ thể của DNC-Chain sẽ kiểm chuẩn lại tại Mục XI.

Bảo mật và riêng tư dữ liệu bổ sung. Phân quyền truy cập tại RPC cho từng loại dữ liệu (dữ liệu công khai, dữ liệu riêng tư, thông tin giao dịch, nhật ký sự kiện); cơ chế xác minh bằng chữ ký số cho yêu cầu truy cập dữ liệu riêng tư; tách biệt quyền sở hữu logic của dữ liệu với lớp lưu trữ vật lý. Chi tiết tại Mục VII.

Tương thích hoàn toàn với EVM. Hợp đồng thông minh viết bằng Solidity triển khai trên DNC-Chain không cần sửa đổi. Các ứng dụng phát triển cho Ethereum và các EVM-chains có thể được chuyển sang DNC-Chain với chi phí điều chỉnh tối thiểu.

Môi trường vận hành tuân thủ pháp lý Việt Nam. Chi tiết tại Mục XII.

V. CƠ CHẾ ĐỒNG THUẬN PROOF OF STAKE - PROOF OF AUTHORITY LAI

Cơ chế đồng thuận là thành phần trung tâm trong thiết kế DNC-Chain, kế thừa cơ chế Proof of Stake (PoS) của Ethereum sau nâng cấp The Merge (tháng 9/2022) và tùy chỉnh thành PoS cấp phép (permissioned) kết hợp yếu tố Proof of Authority (PoA) để đáp ứng yêu cầu về chủ quyền, bảo mật và tuân thủ pháp lý.

1. Cấu trúc PoS-PoA lai

Cơ chế PoS-PoA lai của DNC-Chain kết hợp hai yếu tố bổ sung cho nhau:

- **Proof of Stake (PoS - bằng chứng cổ phần):** Validator đặt cược một lượng token nội bộ tối thiểu để tham gia xác minh. Validator xác minh giao dịch, đề xuất khối và nhận token phần thưởng; đồng thời chịu phạt (slashing) nếu vi phạm quy tắc (xác minh sai, ký hai khối cùng slot, vắng mặt kéo dài).

- **Proof of Authority (PoA - bằng chứng thẩm quyền):** Chỉ validator đã được cơ quan quản trị của thành phố phê duyệt mới tham gia mạng. Danh tính và thẩm quyền của validator xác lập ngoài chuỗi thông qua quyết định của cơ quan có thẩm quyền, ghi vào hợp đồng quản lý cấp phép (Access Control List - ACL) ngay tại khối khởi tạo (genesis block).

Sự kết hợp này khắc phục nhược điểm của từng cơ chế đơn lẻ: PoS thuần dễ bị chi phối bởi đối tượng có tiềm lực tài chính lớn; PoA thuần tập trung quyền lực vào một số ít tổ chức, dễ thông đồng. Cơ chế lai bảo đảm validator vừa có thẩm quyền được công nhận (qua PoA), vừa chịu ràng buộc kinh tế khi vi phạm (qua PoS và cơ chế slashing).

2. Cấu trúc thời gian và quy trình đồng thuận

Cấu trúc thời gian của DNC-Chain: slot time cấu hình linh hoạt 1 - 6 giây (mặc định 3 giây); epoch gồm 32 slot, là đơn vị tổ chức chu kỳ đồng thuận và hoàn tất khối. Cấu hình slot time có thể điều chỉnh theo khối lượng giao dịch thực tế mà không cần dừng mạng.

Quy trình đồng thuận diễn ra theo năm bước:

Bước 1 - Xáo trộn và phân bổ ủy ban (Committee Shuffling). Đầu mỗi epoch, các validator hợp lệ được chọn ngẫu nhiên bằng Verifiable Random Function (VRF) và phân bổ vào các ủy ban xác minh độc lập, bảo đảm chống tấn công dự đoán trước người đề xuất khối.

Bước 2 - Đề xuất khối (Block Proposal). Trong mỗi slot, một validator được chọn làm người đề xuất khối, thu thập giao dịch từ mempool, thực thi trong EVM và tạo khối hợp lệ.

Bước 3 - Xác minh và chứng thực (Attestation). Các validator còn lại xác minh tính hợp lệ của khối (chữ ký, tuân thủ EVM, trạng thái kết quả thống nhất) và phát chữ ký chứng thực.

Bước 4 - Tổng hợp chữ ký (Signature Aggregation). Các chứng thực được tổng hợp thành một chữ ký BLS (Boneh-Lynn-Shacham) duy nhất đại diện sự đồng thuận của ủy ban, giảm dữ liệu truyền và tăng hiệu quả.

Bước 5 - Hoàn tất khối (Finalization). Áp dụng cơ chế Casper Friendly Finality Gadget (FFG) của Ethereum: khối được coi là hoàn tất khi có ít nhất 2/3 tổng số validator xác nhận qua hai epoch liên tiếp. Sau khi hoàn tất, khối không thể bị đảo ngược trừ khi hơn 1/3 tổng số cổ phần bị chiếm quyền - điều không khả thi trong mạng có cấp phép.

3. Chuyển đổi PoS không cấp phép sang PoS cấp phép

Chuyển đổi từ PoS công khai sang PoS cấp phép thực hiện qua bốn cấu phần:

Tổ chức được cấp phép (Whitelisted Entities). Chỉ validator và RPC node được cấp quyền mới tham gia đồng thuận và vận hành mạng. Danh sách xác lập bằng quyết định của cơ quan có thẩm quyền.

Smart contract quản lý cấp phép. Cơ chế cấp phép validator triển khai qua smart contract chứa Access Control List (ACL) tại genesis block, bảo đảm minh bạch và phân quyền tham gia. Mọi thay đổi danh sách validator thực hiện qua hợp đồng quản trị ValidatorRegistry với cơ chế đa ký và timelock 48 giờ.

Kết nối mạng có kiểm soát. Validator chỉ chấp nhận kết nối peering từ các node tin cậy nằm trong danh sách ACL, giảm tối đa rủi ro tấn công mạng.

Đa dạng phần mềm máy khách. Cơ chế cấp phép và quản trị peering được tùy chỉnh trực tiếp trên các client consensus Prysm và Lighthouse, kết hợp client execution Geth với RPC tùy chỉnh. Việc sử dụng đa dạng client trên cùng một mạng bảo đảm lỗi phần mềm của một client không làm gián đoạn toàn bộ hệ thống. Đây là đặc điểm đã được **VNIDChain áp dụng**, giúp đạt tính ổn định và khả năng phục hồi cao.

4. Ủy ban đồng bộ và cơ chế phạt

Ngoài các ủy ban xác minh chính, DNC-Chain kế thừa cơ chế ủy ban đồng bộ (Sync Committees) của Ethereum, gồm các nhóm validator được chọn ngẫu nhiên thay đổi mỗi 256 epoch. Các ủy ban này cung cấp chữ ký cho mỗi khối, giúp các máy khách nhẹ (light client) đồng bộ dữ liệu nhanh mà không cần tải toàn bộ blockchain.

Validator vi phạm quy tắc đồng thuận (ký khối không hợp lệ, ký hai khối cùng slot, vắng mặt kéo dài) chịu phạt một phần cổ phần đã đặt cược theo cơ chế slashing của Ethereum. Mức phạt tăng dần theo mức độ vi phạm, từ trừ phần thưởng khối đến trừ một phần cổ phần đáng kể và loại khỏi mạng. Cơ chế phạt tạo động lực kinh tế buộc validator vận hành đúng quy tắc, bổ sung cho cơ chế quản trị hành chính của PoA.

VI. MÔ HÌNH NODE VÀ LỘ TRÌNH MỞ RỘNG

1. Phân loại node theo vai trò

DNC-Chain tổ chức mạng theo ba loại node với vai trò kỹ thuật phân biệt:

Node quản trị mạng (Admin Node) điều phối cấu hình mạng, quản lý danh sách node được cấp phép, phê duyệt thay đổi thành phần mạng, kiểm soát trạng thái vận hành chung. Node quản trị không tham gia trực tiếp vào cơ chế đồng thuận tạo khối; đóng vai trò điều khiển và giám sát.

Validator Node xác minh giao dịch, tham gia đồng thuận PoS-PoA, đề xuất và chứng thực khối, duy trì trạng thái sổ cái. Đây là nhóm node cốt lõi bảo đảm tính toàn vẹn và liên tục của chuỗi.

Node hỗ trợ kỹ thuật (Service Node) hỗ trợ giám sát, tích hợp, sao lưu, phục hồi, kết nối và các chức năng kỹ thuật phục vụ vận hành mạng; có thể bao gồm node chỉ đọc phục vụ truy vấn, full node phục vụ sao lưu và gateway node phục vụ tích hợp.

2. Cấu hình node theo giai đoạn

DNC-Chain bố trí phân tán tại tối thiểu 03 địa điểm độc lập, với cấu hình node tăng theo lộ trình triển khai các sản phẩm ứng dụng:

Bảng A.4. Cấu hình node tối thiểu theo giai đoạn

Giai đoạn	Loại node	Số lượng	Địa điểm bố trí	Vai trò
-----------	-----------	----------	-----------------	---------

Giai đoạn	Loại node	Số lượng	Địa điểm bố trí	Vai trò
2026 - 2027	Node quản trị mạng	01	01 cơ sở nhà nước độc lập	Điều phối cấu hình mạng, quản lý danh sách node được cấp phép, phê duyệt thay đổi thành phần mạng, kiểm soát trạng thái vận hành chung
2026 - 2027	Validator node	01	Hạ tầng nhà nước phù hợp theo phương án được phê duyệt	Xác minh giao dịch, tham gia đồng thuận, tạo khối, duy trì trạng thái sổ cái
2026 - 2027	Node hỗ trợ kỹ thuật / Service node	02	Trung tâm dữ liệu doanh nghiệp trên địa bàn thành phố đáp ứng điều kiện kỹ thuật, an toàn, an ninh	Hỗ trợ giám sát, tích hợp, sao lưu, phục hồi, kết nối và các chức năng kỹ thuật phục vụ vận hành mạng
Đến 2030	Node quản trị mạng	02	02 cơ sở nhà nước độc lập	Duy trì cơ chế quản trị mạng có cấp phép, kiểm soát cấu hình, quản lý thành viên mạng
Đến 2030	Validator node	02	Tối thiểu 01 vị trí hạ tầng nhà nước; 01 validator còn lại tại hạ tầng đáp ứng điều kiện kỹ thuật theo phương án được phê duyệt	Xác minh giao dịch, mở rộng khả năng vận hành, tăng dự phòng và nâng cao tính sẵn sàng
Đến 2030	Node hỗ trợ kỹ thuật / Service node	02	Hạ tầng doanh nghiệp hoặc hạ tầng phù hợp theo phương án được phê duyệt	Hỗ trợ giám sát, tích hợp, sao lưu, phục hồi, kết nối và bảo đảm vận hành kỹ thuật toàn mạng

Cấu hình giai đoạn 2026 - 2027 gồm 04 node tổng (01 quản trị + 01 validator + 02 service), phù hợp quy mô khối lượng giao dịch dự kiến của các sản phẩm Tầng 1 (SP1, SP2) trong giai đoạn khởi tạo hạ tầng. Cấu hình đến 2030 gồm 06 node (02 quản trị + 02 validator + 02 service), đáp ứng khối lượng giao dịch của 10 sản phẩm ứng dụng khi vận hành đồng thời, bao gồm các sản phẩm Tầng 4 gắn với IFC.

3. Cơ chế mở rộng mạng

Trong các giai đoạn tiếp theo sau 2030, căn cứ số lượng ứng dụng tiếp nhận, nhu cầu xử lý giao dịch, điều kiện hạ tầng và yêu cầu bảo đảm tính sẵn sàng, thành phố xem xét mở rộng thêm validator node và node hỗ trợ kỹ thuật. Tham chiếu cấu hình kiểm chuẩn của VNIDChain (06 full node đạt 5.000 TPS trung bình, 20.000 TPS đỉnh) cho thấy mạng cùng mô hình kiến trúc đạt mục tiêu hiệu năng đến 2030 với quy mô 06 node;

địa mở rộng lý thuyết của DNC-Chain là 58.000 - 100.000 TPS khi tăng quy mô validator và áp dụng các giải pháp mở rộng đã xác định tại Mục X.

Mở rộng thực hiện qua hợp đồng quản trị ValidatorRegistry với đa ký và timelock, không làm thay đổi nguyên tắc quản trị mạng, không phát sinh kiến trúc phân tán thiếu kiểm soát, không yêu cầu dừng mạng. Đối với node do doanh nghiệp vận hành, cơ quan đầu mối quản lý hạ tầng duy trì phương án dự phòng kỹ thuật, cập nhật và kiểm tra định kỳ, gắn với kế hoạch sao lưu, phục hồi của toàn hệ thống.

VII. QUẢN TRỊ TRUY CẬP DỮ LIỆU, BẢO MẬT VÀ QUẢN LÝ KHOÁ

1. Xác minh điểm cuối và phân quyền truy cập dữ liệu

DNC-Chain yêu cầu xác minh danh tính tại mọi điểm truy cập RPC và block explorer. Cơ chế xác minh sử dụng chữ ký số theo chuẩn ERC-191 hoặc quy chuẩn tương đương do Ban Cơ yếu Chính phủ chấp thuận, bảo đảm tính xác minh và toàn vẹn của mọi yêu cầu truy cập.

Dữ liệu trên DNC-Chain được phân loại và phân quyền truy cập theo năm cấp độ:

- **Dữ liệu công khai (Public Data):** truy cập tự do bởi mọi người dùng.
- **Dữ liệu riêng tư (Private Data):** chỉ truy cập khi có xác minh hợp lệ của người dùng sở hữu dữ liệu.
- **Thông tin giao dịch (Transaction Data):** chỉ hiển thị cho các bên liên quan trực tiếp (địa chỉ gửi, địa chỉ nhận, các địa chỉ xuất hiện trong trường dữ liệu giao dịch).
- **Nhật ký sự kiện (Events & Logs):** chỉ hiển thị cho các địa chỉ có trong event topics hoặc data field.
- **Dữ liệu chi tiết giao dịch (tx.data):** chỉ khả dụng cho bên gửi.

DNC-Chain áp dụng đồng thời cơ chế RBAC (Role-Based Access Control) tổ chức theo bốn lớp phân cấp: vai trò mạng, vai trò tổ chức, vai trò ứng dụng, vai trò dịch vụ. Chi tiết định nghĩa, quy trình cấp, thu hồi và kế thừa giữa các lớp được đặc tả tại Mô đun 3 (Phần B). Mọi thao tác on-chain đi qua kiểm tra quyền trước khi thực thi; kết quả kiểm tra ghi vào nhật ký bất biến phục vụ kiểm toán.

2. Bảo mật lưu trữ

Hệ thống lưu trữ của DNC-Chain thiết kế để tách biệt quyền sở hữu logic của dữ liệu với lớp lưu trữ vật lý, bảo vệ người dùng trước nguy cơ truy cập trái phép từ tầng lưu trữ thấp. Trong blockchain công khai, khoá lưu trữ không gắn trực tiếp với chủ sở hữu; DNC-Chain khắc phục bằng cách phân tách dữ liệu theo "logical owner" được xác định bởi mã hợp đồng ứng dụng (application contract code). Quyền truy cập dữ liệu của người dùng được bảo đảm bằng chữ ký số.

Toàn bộ cơ sở dữ liệu của các node (LevelDB hoặc RocksDB) mã hóa bằng AES-256 với khoá do HSM quản lý. Nhật ký giao dịch và trạng thái mã hoá riêng biệt.

Sao lưu toàn trạng thái blockchain thực hiện chu kỳ 24 giờ, lưu tại 03 địa điểm độc lập: Trung tâm Dữ liệu thành phố Đà Nẵng, một địa điểm dự phòng ngoài thành phố theo

thỏa thuận, và một bản sao ngoại tuyến. Thời gian phục hồi sau sự cố (RTO) không quá 04 giờ; mất dữ liệu tối đa cho phép (RPO) không quá 15 phút.

3. Quản lý khoá mật mã và HSM

Khóa mật mã của validator, node quản trị và các cơ quan phát hành bằng chứng được quản lý theo ba cấp độ:

- **Phần cứng chuyên dụng.** Khóa riêng lưu trong Hardware Security Module (HSM). Ưu tiên sử dụng thiết bị mật mã do doanh nghiệp, tổ chức Việt Nam sản xuất đã được Ban Cơ yếu Chính phủ chứng nhận đạt quy chuẩn tương đương FIPS 140-3 Level 3 (chuẩn của Viện Tiêu chuẩn và Công nghệ Hoa Kỳ - NIST đã thay thế FIPS 140-2 từ ngày 22/9/2021). Trường hợp thị trường trong nước chưa có sản phẩm đáp ứng yêu cầu kỹ thuật cụ thể, có thể sử dụng HSM nhập khẩu đạt chuẩn FIPS 140-3 Level 3 hoặc đang trong giai đoạn chuyển tiếp với chứng nhận FIPS 140-2 Level 3 còn hiệu lực. Khóa không tồn tại ngoài HSM dưới dạng rõ. Giao tiếp giữa phần mềm và HSM tuân thủ chuẩn PKCS#11. Vòng đời khóa tuân thủ chuẩn ISO/IEC 11770 về quản lý khóa mật mã.

- **Sao lưu theo cơ chế Shamir Secret Sharing.** Khóa gốc của Ủy ban nhân dân thành phố và các cơ quan chủ trì chia thành n phần, cần tối thiểu m phần để phục hồi. Áp dụng cấu hình 3-of-5 cho khóa gốc; các phần sao lưu đặt tại HSM ở các cơ sở nhà nước khác nhau.

- **Luân phiên khóa định kỳ.** Khóa ký giao dịch luân phiên 12 tháng/lần hoặc khi phát hiện bất thường. Khóa mới tạo trong HSM trước khi khóa cũ hết hạn 30 ngày; quá trình chuyển đổi có nghi thức ký (key ceremony) với giám sát của đại diện các cơ quan.

4. Va chạm khóa và theo dõi mật mã hậu lượng tử

Cấu trúc khóa lưu trữ hiện sử dụng 20 byte cho địa chỉ chủ sở hữu và 12 byte cho không gian khóa, về mặt lý thuyết có khả năng chịu tấn công va chạm khóa (key collision). Trên thực tế, do mỗi lần sửa đổi khóa đều được xác minh bởi chủ sở hữu, đối tượng tấn công chỉ có thể tác động đến khóa do chính đối tượng đó kiểm soát, không thể ảnh hưởng đến khóa của chủ thể khác. Việc tấn công vét cạn keccak256 để tạo địa chỉ hợp đồng mới trùng khóa 96-bit hiện có là không khả thi về mặt tính toán do độ phức tạp tính toán vượt năng lực phần cứng hiện hành.

DNC-Chain theo dõi tiến trình chuẩn hóa mật mã hậu lượng tử của National Institute of Standards and Technology (NIST) Hoa Kỳ, bao gồm các thuật toán CRYSTALS-Kyber (trao đổi khóa) và CRYSTALS-Dilithium (chữ ký số), cũng như tiến trình ban hành quy chuẩn tương ứng của Ban Cơ yếu Chính phủ. Một giải pháp hậu lượng tử tiềm năng là đăng ký rằng một khóa (12 byte) thuộc về hợp đồng ứng dụng đầu tiên được biết đến, chỉ tồn tại một khe lưu trữ mỗi hợp đồng nhưng ngăn chặn hiệu quả mọi tấn công va chạm khóa trong môi trường hậu lượng tử. Việc triển khai mật mã hậu lượng tử thực hiện khi: (i) Ban Cơ yếu Chính phủ ban hành quy chuẩn tương ứng; (ii) các client Ethereum đã hỗ trợ ổn định các thuật toán này; (iii) có đánh giá rủi ro cho thấy lợi ích vượt chi phí triển khai.

VIII. LIÊN THÔNG ĐA CHUỖI

1. Nguyên tắc và phạm vi

DNC-Chain bảo đảm liên thông với các mạng blockchain khác thông qua Mô đun Cầu nối đa chuỗi (Mô đun 1 - Phần B). Liên thông tuân thủ năm nguyên tắc: (i) có kiểm soát qua allowlist được phê duyệt; (ii) không hợp nhất sổ cái; (iii) không chuyển giao tài sản mã hoá xuyên chuỗi trên hạ tầng dùng chung; (iv) có giám sát và cơ chế ngắt kết nối khẩn cấp; (v) mạng xác minh thông điệp do cơ quan, tổ chức Việt Nam vận hành.

Phạm vi đối tượng liên thông bao gồm Nền tảng blockchain quốc gia khi chuẩn kết nối chính thức được công bố; các blockchain cấp phép của bộ, ngành, địa phương khác khi có nhu cầu liên thông thực tiễn; các blockchain công khai quốc tế theo phê duyệt của cơ quan có thẩm quyền trong phạm vi hạn chế.

2. Cơ chế kỹ thuật

Liên thông thực hiện qua ba loại thao tác: (i) truyền thông điệp liên chuỗi (Cross-Chain Messaging) qua các giao thức Relay/Bridge - chuyển thông điệp, bằng chứng mật mã (Merkle Proof), chứng nhận xác minh (Verifiable Credential) mà không di chuyển dữ liệu nhạy cảm; (ii) chia sẻ danh mục tin cậy (Shared Trust Registry) - chia sẻ có kiểm soát danh mục node, danh tính tổ chức vận hành và chính sách đồng thuận với mạng đối tác được phê duyệt; (iii) xác minh bằng chứng độc lập - xác minh bằng chứng đến từ chuỗi khác dựa trên Merkle Proof và VC Proof, không sao chép toàn bộ dữ liệu nghiệp vụ.

Mạng xác minh thông điệp liên chuỗi của DNC-Chain vận hành bởi các cơ quan, tổ chức Việt Nam được phê duyệt (các cơ quan nhà nước của thành phố Đà Nẵng, cơ quan chuyên trách về an toàn thông tin thuộc Bộ Khoa học và Công nghệ, Ban Cơ yếu Chính phủ và các đối tác được phê duyệt khác), không phụ thuộc vào mạng xác minh công khai quốc tế trong vai trò xác minh chính.

3. Kiểm soát quản trị

Mọi thay đổi danh sách chuỗi được phép kết nối, danh sách bên xác minh và tham số liên chuỗi thực hiện qua hợp đồng quản trị WhitelistRegistry với đa ký tối thiểu 3/5 của các cơ quan quản trị mạng và timelock 48 giờ. Cơ chế CircuitBreaker tự động ngắt kết nối khi phát hiện bất thường (quá tải, khối lượng giao dịch vượt ngưỡng, sai lệch dữ liệu giữa các bên xác minh); khôi phục kết nối yêu cầu phê duyệt đa ký. Việc phê duyệt bổ sung chuỗi kết nối ngoài phạm vi thành phố thuộc thẩm quyền của Ủy ban nhân dân thành phố; phê duyệt chuỗi kết nối trong phạm vi thành phố thuộc thẩm quyền Sở Khoa học và Công nghệ theo Quy chế vận hành DNC-Chain. Toàn bộ thao tác quản trị liên thông ghi nhật ký bất biến trên chuỗi phục vụ kiểm toán theo Luật An toàn thông tin mạng số 86/2015/QH13 và Luật An ninh mạng số 24/2018/QH14.

IX. ĐỊNH DANH PHI TẬP TRUNG VÀ TÍCH HỢP VNeID

1. Mô hình định danh ba lớp

DNC-Chain áp dụng mô hình định danh ba lớp phục vụ xác minh chủ thể mà không ghi dữ liệu cá nhân lên chuỗi bất biến:

Lớp 1 - Định danh gốc tại hệ thống quốc gia. Đối với cá nhân, sử dụng Hệ thống định danh điện tử quốc gia VNeID do Bộ Công an quản lý. Đối với tổ chức, sử dụng Hệ thống đăng ký doanh nghiệp quốc gia hoặc hệ thống đăng ký của cơ quan chủ quản.

Lớp 2 - Định danh phi tập trung trên DNC-Chain. Dựa trên chuẩn Decentralized Identifier (DID) của World Wide Web Consortium (W3C). Mỗi chủ thể sau xác minh tại Lớp 1 được cấp một DID duy nhất dưới dạng mã vô danh trên DNC-Chain (Hub ID), kèm một hoặc nhiều Verifiable Credential (VC) dạng chứng thư số. Chủ thể tự quản lý khoá riêng tương ứng với DID.

Lớp 3 - Xác minh ứng dụng. Khi tương tác với sản phẩm ứng dụng, chủ thể xuất trình VC phù hợp để chứng minh thuộc tính cần thiết (ví dụ: đã xác minh VNeID Mức 2 theo Nghị định số 69/2024/NĐ-CP, là cán bộ cơ quan nhà nước, đã tốt nghiệp đại học). Ứng dụng xác minh chữ ký của cơ quan cấp VC và thời hạn hiệu lực; không truy vấn lại Lớp 1 trong từng giao dịch.

2. Luận cứ và cơ chế bảo vệ dữ liệu cá nhân

Luận cứ pháp lý. Việt Nam đã có VNeID được pháp luật công nhận làm định danh gốc của công dân. Mô hình DID - VC tận dụng VNeID làm lớp xác minh gốc, bảo đảm tính pháp lý và tránh xung đột với chính sách định danh của Nhà nước; không hình thành hệ thống định danh công dân riêng thay thế VNeID.

Luận cứ bảo vệ dữ liệu cá nhân. Ghi thông tin cá nhân trực tiếp lên blockchain không phù hợp Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 do tính bất biến xung đột với quyền xóa dữ liệu. Mô hình DID - VC cho phép chủ thể được xác minh bởi VNeID ở hệ thống nguồn, trên chuỗi chỉ lưu DID vô danh và giá trị băm của VC; quyền xóa dữ liệu cá nhân được bảo đảm qua cơ chế thu hồi VC.

Luận cứ kiểm toán. Mọi giao dịch trên DNC-Chain truy xuất được về DID. Khi có yêu cầu pháp lý hợp lệ, DID có thể truy ngược về chủ thể thực tại hệ thống nguồn qua Mô đun 7, phục vụ điều tra, kiểm toán theo đúng quy định.

3. Các loại Chứng nhận xác minh trên DNC-Chain

DNC-Chain hỗ trợ ba loại VC chính phục vụ các tình huống xác minh phổ biến trong 10 sản phẩm:

Bảng A.5. Các loại Chứng nhận xác minh

Loại VC	Bên cấp	Nội dung xác nhận	Ví dụ ứng dụng
Identity VC	Hệ thống nguồn được ủy quyền hoặc cơ quan có thẩm quyền (thông qua VNeID)	Mức xác minh VNeID (Mức 1, Mức 2 theo Nghị định số 69/2024/NĐ-CP ngày 25/6/2024 của Chính phủ; trong đó Mức 2 bao gồm sinh trắc học), ngày cấp, thời hạn hiệu lực	Xác minh công dân khi truy cập dịch vụ công trên DNC-Chain

Loại VC	Bên cấp	Nội dung xác nhận	Ví dụ ứng dụng
Organization VC	Hệ thống đăng ký doanh nghiệp; cơ quan chủ quản của tổ chức	Mã số thuế, loại hình tổ chức, quyền tham gia ứng dụng	Doanh nghiệp tham gia sàn giao dịch sở hữu trí tuệ (SP6), sản dữ liệu thành phố (SP5)
Action VC	Hệ thống nghiệp vụ chuyên ngành	Bằng chứng đã hoàn thành bước nghiệp vụ (đã nộp hồ sơ, đã phê duyệt, đã hoàn thành đào tạo)	Xác minh văn bằng trên SP2, xác minh hồ sơ y tế trên SP4

Trên chuỗi chỉ ghi: DID vô danh của chủ thể, giá trị băm của VC, siêu dữ liệu tối thiểu (cơ quan cấp, loại VC, thời hạn). Không ghi trực tiếp bất kỳ trường dữ liệu cá nhân nào. Quyền xóa thực hiện qua thu hồi VC trong hợp đồng RevocationRegistry, đạt hiệu quả tương đương về mặt pháp lý và thực tiễn.

X. MỞ RỘNG VÀ ỨNG DỤNG ZERO-KNOWLEDGE

1. Mục tiêu và phạm vi ứng dụng Zero-Knowledge

DNC-Chain kế thừa các giải pháp mở rộng mã nguồn mở của hệ sinh thái Ethereum (Optimistic Rollups, ZK-Rollups, Validium), được đề xuất trong các định hướng phát triển tương lai của Ethereum. Trên nền tảng đó, DNC-Chain định hướng phát triển các Ứng dụng Không Tiết lộ Tri Thức (Zero-Knowledge Applications) phục vụ các nghiệp vụ đặc thù của thành phố có yêu cầu bảo mật và xác minh dữ liệu cao.

Các ZK Circuit chuyên dụng được thiết kế để đáp ứng các mục tiêu: mở rộng lưu lượng dữ liệu truy vết cho các sản phẩm khối lượng lớn (đặc biệt SP3 - Digital Twin); cung cấp dữ liệu có thể xác minh bằng chứng mật mã trước khi ghi lên chuỗi; duy trì bảo mật giao dịch trong khi vẫn xác minh được tính đúng đắn. Ví dụ cụ thể trong bối cảnh 10 sản phẩm của Đề án: chứng minh "trên 18 tuổi" mà không tiết lộ ngày sinh cụ thể trong giao dịch SP1; chứng minh "có bằng đại học đúng chuyên ngành" mà không cần cung cấp toàn bộ nội dung bằng cấp trong SP2.

2. Điều kiện kích hoạt và tham chiếu chuẩn kỹ thuật

Triển khai ZK Applications trên DNC-Chain thực hiện theo cơ chế tùy chọn, áp dụng khi đồng thời thỏa mãn ba điều kiện: (i) có yêu cầu nghiệp vụ cụ thể của cơ quan chủ trì sản phẩm và được phê duyệt bằng văn bản; (ii) có công cụ mã nguồn mở đã trưởng thành (các hệ chứng minh Groth16, PLONK, Halo2 đã ổn định, đã qua kiểm toán nhiều vòng và có triển khai khu vực công tham chiếu); (iii) có đánh giá tác động cho thấy lợi ích vượt chi phí triển khai và chi phí kiểm toán mạch (circuit audit). Trong giai đoạn 2026 - 2030, ZK không phải cấu phần bắt buộc cho mọi giao dịch trên DNC-Chain; ưu tiên áp dụng ở dạng ZK Application cho từng nghiệp vụ cụ thể, không triển khai ZK-Rollup ở cấp Layer-2 trong giai đoạn này.

XI. KIỂM CHUẨN HIỆU NĂNG

1. Mục tiêu thiết kế

Bảng A.6. Mục tiêu kỹ thuật hiệu năng của DNC-Chain

Chỉ tiêu	Mục tiêu đến 2030	Căn cứ tham chiếu
Thông lượng trung bình	5.000 TPS	Kết quả kiểm chuẩn VNIDChain trên cùng mô hình Permissioned Ethereum + PoS-PoA
Thông lượng đỉnh	20.000 TPS	Đạt được khi áp dụng đồng thời batching, pipelining giao dịch và tối ưu hoá tham số validator
Dur địa mở rộng	58.000 - 100.000 TPS	Khi mở rộng validator trong các giai đoạn sau 2030
Thời gian khối (slot time)	3 giây mặc định, cấu hình linh hoạt 1 - 6 giây	Đặc tính kỹ thuật Permissioned Ethereum
Thời gian hoàn tất khối (finality)	1,5 - 2 blocks	Casper FFG
Độ trễ xác nhận giao dịch	1 - 2 giây	Đặc tính kỹ thuật Permissioned Ethereum
Thời gian sẵn sàng của mạng	≥ 99,9% theo tháng	Cam kết vận hành
Thời gian phục hồi sau sự cố (RTO)	≤ 04 giờ	Theo Mục VII; tham chiếu chuẩn ISO 22301 về quản lý liên tục hoạt động
Mất dữ liệu tối đa cho phép (RPO)	≤ 15 phút	Theo Mục VII; tham chiếu chuẩn ISO 22301

Các mục tiêu trên đặt trên cơ sở tham chiếu kết quả kiểm chuẩn đã công bố của VNIDChain (cùng mô hình Permissioned Ethereum + PoS-PoA): thông lượng trung bình 5.000 TPS, đỉnh 20.000 TPS, trên cấu hình 06 full node với thông số phần cứng trung bình (CPU 8 nhân, RAM 32GB, SSD 1TB). Kết quả thực tế của DNC-Chain phụ thuộc cấu hình hạ tầng, điều kiện vận hành và đặc thù ứng dụng cụ thể; được kiểm chuẩn thực nghiệm trước nghiệm thu và định kỳ trong quá trình vận hành.

2. Phương pháp kiểm chuẩn

Kiểm chuẩn hiệu năng DNC-Chain thực hiện theo ba chu kỳ:

Kiểm chuẩn nghiệm thu ban đầu trước khi đưa hạ tầng vào vận hành chính thức, trên cấu hình hạ tầng thật. Đo các chỉ tiêu: thông lượng trung bình và đỉnh; độ trễ xác nhận giao dịch (percentile 50, 95, 99); mức tiêu thụ tài nguyên (CPU, bộ nhớ, băng thông); khả năng phục hồi sau khi node offline.

Kiểm chuẩn định kỳ thực hiện 06 tháng/lần trong quá trình vận hành, so sánh với kiểm chuẩn nghiệm thu ban đầu để phát hiện suy giảm hiệu năng.

Kiểm chuẩn sau thay đổi lớn thực hiện sau mỗi lần nâng cấp phần mềm lõi, thay đổi cấu hình mạng, bổ sung hoặc thay thế validator. Phát hiện sớm lỗi quy hiệu năng.

3. Tham số kiểm chuẩn đại diện

Tham số kiểm chuẩn đại diện của DNC-Chain dự kiến:

Phần cứng validator node: CPU 8 nhân, RAM 32GB, SSD 1 TB với 4000 IOPS và throughput 125 MB/s, băng thông kết nối $\geq 300\text{Mbps}$ trong nước;

Hệ điều hành: Linux Ubuntu LTS;

Bộ công cụ giám sát: Prometheus (agent mode), Mimir, Loki, Tempo, Grafana;

Tham số mạng: slot time 3 giây (mặc định), epoch 32 slot, gas limit 100M - 1B Gwei;

Giao dịch thử nghiệm: native transfer, ERC-20 token transfer, giao dịch ghi bằng chứng (hash write);

Baseline đối chiếu: Ethereum mainnet (20 TPS trên L1, 220 TPS cả L1 và L2, finality 2 epoch tương đương 12 phút).

Công cụ kiểm chuẩn sử dụng các công cụ mã nguồn mở chuẩn ngành (Hyperledger Caliper, chainhammer hoặc tương đương). Kết quả ghi nhận trong hệ thống giám sát và báo cáo định kỳ tới Sở Khoa học và Công nghệ; công bố trong phạm vi cho phép.

XII. TUÂN THỦ PHÁP LÝ VÀ TIÊU CHUẨN KỸ THUẬT

1. Văn bản pháp lý tuân thủ

Bảng A.7. Văn bản pháp lý tuân thủ của DNC-Chain

Văn bản pháp lý	Yêu cầu chính	Cơ chế đáp ứng
Luật Giao dịch điện tử số 20/2023/QH15	Chữ ký số, thông điệp dữ liệu có giá trị pháp lý	Chữ ký ECDSA tương thích chuẩn; tích hợp chứng thư số công cộng; ghi dấu thời gian trên chuỗi

Văn bản pháp lý	Yêu cầu chính	Cơ chế đáp ứng
Luật Dữ liệu số 60/2024/QH15	Quản lý dữ liệu tại hệ thống nguồn, kết nối chia sẻ có kiểm soát	DNC-Chain không lưu dữ liệu nghiệp vụ gốc; kết nối qua LGSP; nhật ký truy vấn đầy đủ
Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15	Tối thiểu hoá dữ liệu, quyền xóa, quyền truy cập	Không ghi dữ liệu cá nhân lên chuỗi; quyền xóa thực hiện qua thu hồi VC; Mô đun 7 bảo đảm tách định danh
Luật An toàn thông tin mạng số 86/2015/QH13 (được sửa đổi, bổ sung bởi Luật số 35/2018/QH14; bị hợp nhất, thay thế bởi Luật An ninh mạng số 116/2025/QH15 kể từ ngày 01/7/2026)	Bảo vệ hệ thống thông tin theo cấp độ	Phân cấp độ theo quy định; hệ thống SOC; quy trình ứng cứu sự cố;
Luật An ninh mạng số 24/2018/QH14 và Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025 (có hiệu lực thi hành kể từ ngày 01/7/2026, hợp nhất và thay thế Luật ATTT mạng số 86/2015/QH13 và Luật ANM số 24/2018/QH14)	Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng	Phối hợp với cơ quan chuyên trách; kiểm tra định kỳ
Nghị định số 278/2025/NĐ-CP	Kết nối, chia sẻ dữ liệu giữa cơ quan nhà nước	Kết nối qua LGSP theo chuẩn chung; không kết nối trực tiếp từ hệ thống nguồn
Nghị định số 356/2025/NĐ-CP	Hướng dẫn Luật Bảo vệ dữ liệu cá nhân	Cơ chế thu hồi VC; đánh giá tác động xử lý dữ liệu; nhật ký truy vấn
Luật Căn cước số 26/2023/QH15 ngày 27/11/2023	Cơ sở pháp lý về căn cước công dân và định danh điện tử	DNC-Chain tích hợp định danh dựa trên VNeID và Cơ sở dữ liệu quốc gia về dân cư do Bộ Công an quản lý; không xây dựng định danh công dân độc lập song song với hệ thống quốc gia

Văn bản pháp lý	Yêu cầu chính	Cơ chế đáp ứng
Luật Định danh và xác thực điện tử số 91/2024/QH15 ngày 29/11/2024 và Nghị định số 69/2024/NĐ-CP ngày 25/6/2024	Tài khoản định danh điện tử Mức 1, Mức 2; quyền và nghĩa vụ chủ thể	Mô đun 7 chỉ nhận mức xác minh VNeID, không lưu thông tin cá nhân; tích hợp qua OpenID Connect
Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 và TCVN 11930:2017 về yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ	Bảo đảm an toàn hệ thống thông tin theo cấp độ	Node validator và service node đặt tại trung tâm dữ liệu đạt cấp độ 3 trở lên theo TCVN 11930:2017; hồ sơ phương án bảo đảm an toàn thông tin được phê duyệt; áp dụng kết hợp các tiêu chuẩn quốc tế chuyên ngành chuỗi khối theo Mục XII.2
Luật Phòng, chống rửa tiền số 14/2022/QH15 ngày 15/11/2022	Phòng chống rửa tiền, chống tài trợ khủng bố đối với tài sản mã hoá	DNC-Chain hỗ trợ kỹ thuật giám sát thời gian thực, đối soát giao dịch cho cơ quan có thẩm quyền (SP8, SP9, SP10 Tầng 4 gần IFC/sandbox); không trực tiếp thực hiện nghĩa vụ AML/CFT thuộc thẩm quyền doanh nghiệp vận hành
Nghị quyết số 136/2024/QH15 ngày 26/6/2024 và Nghị quyết số 259/2025/QH15 ngày 11/12/2025 của Quốc hội	Cơ chế đặc thù phát triển thành phố Đà Nẵng; thí điểm chính sách công nghệ blockchain	Cơ sở pháp lý để thành phố cấp phép, quản trị DNC-Chain trong phạm vi thẩm quyền địa phương
Quyết định số 2439/QĐ-TTg ngày 04/11/2025 của Thủ tướng Chính phủ	Khung kiến trúc dữ liệu quốc gia, Khung quản trị, quản lý dữ liệu quốc gia (phiên bản 1.0)	Chuẩn dữ liệu đầu vào và siêu dữ liệu của Mô đun 2 và các sản phẩm tuân thủ Khung kiến trúc dữ liệu quốc gia
Quyết định số 1131/QĐ-TTg ngày 12/6/2025 (được thay thế bởi Quyết định số 21/2026/QĐ-TTg ngày 30/4/2026 có hiệu lực từ 01/7/2026) và Quyết định số 2815/QĐ-TTg ngày 28/12/2025 của Thủ tướng Chính phủ	Danh mục công nghệ chiến lược; Chương trình khoa học, công nghệ và đổi mới sáng tạo quốc gia phát triển sản phẩm công nghệ chiến lược ưu tiên triển khai nhanh	Blockchain (bao gồm DNC-Chain) là công nghệ chiến lược; ưu tiên doanh nghiệp Việt Nam triển khai, làm chủ công nghệ lõi
Quy chuẩn mật mã dân sự của Ban Cơ yếu Chính phủ	Thuật toán mật mã được phép sử dụng trong giao dịch của cơ quan nhà	HSM đạt quy chuẩn; thuật toán tương thích; luân phiên khoá định kỳ

Văn bản pháp lý	Yêu cầu chính	Cơ chế đáp ứng
	nước	

2. Tiêu chuẩn kỹ thuật tham chiếu

DNC-Chain tham chiếu và tuân thủ các tiêu chuẩn kỹ thuật quốc tế và quốc gia sau:

Về kiến trúc tham chiếu chuỗi khối: ISO 23257:2022 (Công nghệ chuỗi khối và sổ cái phân tán - Kiến trúc tham chiếu); các tiêu chuẩn của Ban Kỹ thuật ISO/TC 307 về Chuỗi khối và Sổ cái Phân tán đối với khả năng liên thông, quản trị rủi ro chuỗi khối và kiểm toán mã nguồn hợp đồng thông minh (smart contract audit).

Về blockchain và công nghệ sổ cái phân tán: ISO/TR 23249:2022 (Tổng quan các hệ thống DLT cho quản lý danh tính); ISO/TR 23635 (Hướng dẫn quản trị); ISO/TR 23244 (Tính riêng tư và bảo vệ thông tin cá nhân); ISO/TR 23455 (Tổng quan hợp đồng thông minh và tương tác); ISO/TR 23576 (An toàn của bên giữ tài sản số); ISO/TR 6039 (Xác định chủ thể và khách thể).

Về quản lý an toàn thông tin: ISO/IEC 27001 (Hệ thống quản lý an toàn thông tin); ISO/IEC 27017 (An toàn thông tin dịch vụ đám mây); ISO/IEC 27018 (Bảo vệ dữ liệu cá nhân dịch vụ đám mây công cộng); ISO/IEC 11770 (Quản lý khoá mật mã); ISO 22301 (Quản lý liên tục hoạt động - BCM); FIPS 140-3 của Viện Tiêu chuẩn và Công nghệ Hoa Kỳ (Yêu cầu an toàn cho module mật mã) hoặc tiêu chuẩn tương đương do Ban Cơ yếu Chính phủ ban hành.

Về định danh phi tập trung và chứng nhận xác minh: W3C DID Core v1.0 (Decentralized Identifiers); W3C Verifiable Credentials Data Model v2.0 (W3C Recommendation ngày 15/5/2025) là chuẩn hiện hành; các hệ thống đã phát hành Chứng nhận xác minh theo v1.1 được duy trì trong giai đoạn chuyển đổi.

Về kiến trúc doanh nghiệp: Enterprise Ethereum Client Specification v6 và Enterprise Ethereum Permissioned Blockchains Specification v2 của Enterprise Ethereum Alliance.

Về tiêu chuẩn quốc gia: các tiêu chuẩn kỹ thuật quốc gia về blockchain, nền tảng dữ liệu, an toàn thông tin do Bộ Khoa học và Công nghệ ban hành, được cập nhật theo lộ trình hoàn thiện khung tiêu chuẩn quốc gia.

3. Kiểm toán tuân thủ

Kiểm toán tuân thủ thực hiện theo ba cấp độ:

Kiểm toán kỹ thuật đối với mã nguồn các hợp đồng thông minh cốt lõi (ValidatorRegistry, WhitelistRegistry, hợp đồng của 07 mô đun và 10 sản phẩm) trước khi triển khai lên hạ tầng vận hành chính thức, do tổ chức kiểm toán độc lập đủ năng lực thực hiện; kiểm toán lặp lại sau mỗi lần nâng cấp lớn.

Kiểm toán bảo mật đối với toàn bộ hạ tầng kỹ thuật (node, HSM, mạng, cấu hình) định kỳ 12 tháng/lần hoặc sau mỗi sự cố. Kết quả báo cáo cho Sở Khoa học và Công nghệ và cơ quan chuyên trách về an toàn thông tin.

Kiểm toán tuân thủ pháp lý định kỳ 12 tháng/lần, rà soát tuân thủ pháp luật về giao dịch điện tử, dữ liệu, bảo vệ dữ liệu cá nhân, an toàn thông tin đối với DNC-Chain và các ứng dụng kết nối. Kết quả là căn cứ điều chỉnh Quy chế vận hành DNC-Chain và các quy định kỹ thuật liên quan.

PHẦN B: 07 MÔ ĐUN NỀN TẢNG DÙNG CHUNG CỦA DNC-CHAIN

Phần B thuyết minh kỹ thuật của 07 mô đun nền tảng dùng chung. Các nội dung kỹ thuật chi tiết (schema API, tham số cấu hình triển khai, luồng vận hành theo bước) không thuộc phạm vi Phụ lục này và sẽ được đặc tả tại Quy chế vận hành DNC-Chain và hồ sơ thiết kế của từng dự án thành phần.

07 mô đun được tổ chức theo bốn nhóm chức năng phục vụ tra cứu và định khung tham chiếu: (i) nhóm liên thông gồm Mô đun 1 (Cầu nối Đa chuỗi); (ii) nhóm bằng chứng và đối soát gồm Mô đun 2 (Tích hợp, tạo bằng chứng xác minh và đối soát hồ sơ điện tử); (iii) nhóm an toàn và định danh gồm Mô đun 3 (Quản lý khoá và phân quyền) và Mô đun 7 (Hub làm sạch dữ liệu); (iv) nhóm quản trị tài sản, smart contract và ứng dụng gồm Mô đun 4 (Quản lý giao dịch và Token), Mô đun 5 (Quản lý smart contract) và Mô đun 6 (Quản lý ứng dụng và Marketplace). Phân nhóm này phản ánh mạch tổ chức kỹ thuật, không hình thành cấp quản trị mới ngoài 07 mô đun đã được xác định tại Khoản 4 Mục II Chương IV của Đề án.

Các chuẩn kỹ thuật chung (chữ ký số, mật mã, TLS, HSM, chuẩn token), cơ chế bảo mật, cơ chế tuân thủ pháp lý đã được đặc tả tại Phần A và được các mô đun dẫn chiếu, không lặp lại ở từng mô đun. Cơ chế nâng cấp hợp đồng thông minh (Proxy Upgrade Pattern theo ERC-1967 + đa ký + timelock 48 giờ) áp dụng thống nhất cho toàn bộ 07 mô đun.

Mô đun 1 - Cầu nối Đa chuỗi

1.1. Vai trò và chức năng chính

Mô đun 1 là lớp kết nối liên chuỗi của DNC-Chain, thực hiện trao đổi thông điệp, bằng chứng xác minh và trạng thái nghiệp vụ giữa DNC-Chain với các blockchain và nền tảng ngoài phạm vi thành phố khi có nhu cầu thực tiễn và được cấp có thẩm quyền cho phép. Mô đun không phục vụ chuyên giao tài sản xuyên chuỗi và không sao chép dữ liệu nghiệp vụ gốc; chỉ truyền thông điệp, bằng chứng mật mã (Merkle Proof, VC Proof) và siêu dữ liệu phục vụ xác minh, đối soát.

Mô đun 1 triển khai trên nền tảng giao thức Wormhole (giao thức truyền thông điệp xuyên chuỗi mã nguồn mở đã được kiểm toán nhiều vòng), tuy nhiên mạng xác minh vận hành theo mô hình Private Guardian Set do các cơ quan, tổ chức Việt Nam vận hành như

đã nêu tại Phần A Mục VIII, không sử dụng mạng Guardian công khai quốc tế trong vai trò xác minh chính.

Bốn chức năng kỹ thuật chính của Mô đun 1:

- Truyền thông điệp liên chuỗi (Cross-Chain Messaging) có kiểm soát qua danh sách cho phép;
- Xác minh bằng chứng đến từ chuỗi khác dựa trên Merkle Proof và VC Proof, không sao chép dữ liệu gốc;
- Chia sẻ danh mục tin cậy (Shared Trust Registry) có kiểm soát với các mạng đối tác được phê duyệt;
- Ngắt kết nối khẩn cấp (Circuit Breaker) khi phát hiện bất thường.

1.2. Kiến trúc cấu phần

Mô đun 1 gồm 06 hợp đồng thông minh trên DNC-Chain và các cấu phần off-chain tích hợp với mạng Private Guardian Set.

Bảng B.1.1. Hợp đồng thông minh của Mô đun 1

Hợp đồng	Chức năng
BridgeCore	Điều phối luồng gửi - nhận thông điệp liên chuỗi; gọi các hợp đồng khác của mô đun
WhitelistRegistry	Quản lý danh sách chuỗi, hợp đồng và địa chỉ được phép kết nối
MessageVerifier	Xác minh chữ ký của Private Guardian Set, chữ ký của chuỗi gốc, Merkle Proof, VC Proof
ProofRelay	Chuyển tiếp bằng chứng đã xác minh đến hợp đồng đích trên DNC-Chain
FeeManager	Quản lý phí giao dịch liên chuỗi; phân bổ phí vận hành
CircuitBreaker	Ngắt kết nối tự động khi phát hiện bất thường; khôi phục sau khi được phê duyệt

Các chuẩn tuân thủ của hợp đồng: EIP-712 (ký dữ liệu có cấu trúc), ERC-165 (phát hiện interface), EIP-191 (định dạng chữ ký Ethereum).

Cấu phần off-chain gồm các Private Guardian Node do các cơ quan nhà nước Việt Nam vận hành (quan sát sự kiện, xác minh, đồng ký thông điệp) và các Relay chuyển tiếp thông điệp đã đủ chữ ký.

1.3. Quan hệ với các mô đun khác

Mô đun 1 sử dụng cơ chế RBAC của Mô đun 3 để kiểm soát quyền gửi thông điệp, quyền cập nhật allowlist và quyền ngắt kết nối khẩn cấp. Các hợp đồng của Mô đun 1 tuân thủ quy trình phát triển, kiểm toán và quản lý phiên bản của Mô đun 5. Đối với thông điệp liên quan đến giao dịch của người dùng, Mô đun 1 sử dụng Hub ID do Mô đun 7 cấp, không truyền thông tin cá nhân qua cầu nối.

1.4. Giao diện kỹ thuật chính

Bảng B.1.2. Giao diện chính của Mô đun 1

Nhóm giao diện	Đối tượng	Chuẩn xác minh
API nội bộ cho sản phẩm DNC-Chain (gửi, nhận, tra cứu thông điệp, đăng ký sự kiện)	Các sản phẩm SP1 - SP10	JWT + chữ ký số của sản phẩm + mTLS
API quản trị allowlist và cấu hình	Cơ quan quản trị mạng	JWT + đa ký của cơ quan có thẩm quyền
Giao tiếp với Private Guardian Set	Guardian Node của các cơ quan được phê duyệt	Chữ ký ECDSA secp256k1; mTLS

Mọi thông điệp kèm dấu thời gian và số chuỗi duy nhất (nonce) để chống tấn công phát lại. Chi tiết schema API và cấu trúc thông điệp được đặc tả tại hồ sơ thiết kế Mô đun 1.

1.5. Ràng buộc tuân thủ pháp lý

Mô đun 1 tuân thủ các ràng buộc đã nêu tại Phần A Mục VIII (Liên thông đa chuỗi) và Phần A Mục XII (Tuân thủ pháp lý và tiêu chuẩn kỹ thuật). Cụ thể:

- Mọi kết nối ra ngoài phạm vi thành phố phải qua WhitelistRegistry được phê duyệt bằng quyết định của cơ quan có thẩm quyền;
- Không truyền dữ liệu nghiệp vụ gốc, dữ liệu cá nhân qua cầu nối; chỉ truyền giá trị băm, bằng chứng mật mã và dữ liệu tối thiểu cần thiết;
- Nhật ký thông điệp lưu bất biến trên chuỗi phục vụ kiểm toán theo Luật An toàn thông tin mạng số 86/2015/QH13 (được sửa đổi, bổ sung bởi Luật số 35/2018/QH14) và

Luật An ninh mạng số 24/2018/QH14; kể từ ngày 01/7/2026 áp dụng theo Luật An ninh mạng số 116/2025/QH15.

1.6. Cơ chế nâng cấp

Các hợp đồng của Mô đun 1 triển khai theo Proxy Upgrade Pattern. Việc nâng cấp hợp đồng, thay đổi danh sách Guardian, cập nhật danh sách chuỗi trong WhitelistRegistry đều thực hiện qua đa ký tối thiểu 3/5 của các cơ quan quản trị mạng và thời gian chờ (timelock) tối thiểu 48 giờ. Các tham số CircuitBreaker (ngưỡng kích hoạt, chu kỳ khôi phục) có thể điều chỉnh qua cùng cơ chế.

1.7. Chỉ tiêu mức dịch vụ cốt lõi

Bảng B.1.3. Chỉ tiêu mức dịch vụ của Mô đun 1

Chỉ tiêu	Mục tiêu
Thời gian sẵn sàng	$\geq 99,5\%$ hàng tháng
Thời gian xác minh thông điệp (chiều ra hoặc chiều vào)	≤ 10 phút
Tỷ lệ giao dịch liên chuỗi thành công	$\geq 99\%$ (không kể các giao dịch bị chặn bởi allowlist hoặc CircuitBreaker)
Thời gian phát hiện bất thường và kích hoạt CircuitBreaker	≤ 2 phút kể từ khi ngưỡng bị vượt

1.8. Điều kiện triển khai

Private Guardian Set đã được thành lập với tối thiểu 07 Guardian Node do các cơ quan, tổ chức Việt Nam vận hành;

Danh sách chuỗi kết nối ban đầu đã được Ủy ban nhân dân thành phố phê duyệt;

Kiểm toán bảo mật độc lập mã nguồn các hợp đồng hoàn tất trước khi vận hành chính thức;

Quy trình ứng cứu sự cố liên chuỗi đã được ban hành và diễn tập;

Giai đoạn 2026 - 2027 triển khai chức năng liên thông ở mức phục vụ nhu cầu ưu tiên theo Chương IV Mục II điểm 4 của Đề án; giai đoạn 2028 - 2030 hoàn thiện và mở rộng theo danh mục kết nối được phê duyệt.

Mô đun 2 - Tích hợp, tạo bằng chứng xác minh và đối soát hồ sơ điện tử

2.1. Vai trò và chức năng chính

Mô đun 2 là mô đun kỹ thuật trung tâm của DNC-Chain, đóng vai trò lớp trung gian chuyên biệt giữa hệ thống nguồn, nền tảng tích hợp và chia sẻ dữ liệu thành phố (LGSP) và DNC-Chain. Mô đun tiếp nhận dữ liệu từ hệ thống nguồn, chuẩn hoá, tạo bằng chứng mật mã dưới dạng giá trị băm (hash), ghi nhận bằng chứng lên DNC-Chain, trả biên lai xác minh và hỗ trợ đối soát, kiểm chứng khi có yêu cầu.

Mô đun 2 không thay thế sản phẩm ứng dụng, không thay thế hệ thống nguồn, không lưu trữ hồ sơ gốc. Mô đun chỉ xử lý các trường dữ liệu cần xác minh (siêu dữ liệu, mã hồ sơ, trạng thái xử lý, hash nội dung) theo nguyên tắc thu thập tối thiểu, bảo đảm nguyên tắc tại Chương III Mục II điểm 2 của Đề án: Dữ liệu nghiệp vụ được quản lý tại hệ thống nguồn; blockchain chỉ ghi nhận lớp tin cậy số cần thiết.

Bốn chức năng kỹ thuật chính:

- Tạo bằng chứng xác minh (Proof Creation) cho hồ sơ điện tử, giao dịch và sự kiện nghiệp vụ;
- Gom lô bằng chứng (Batching) qua Merkle Tree để tối ưu chi phí gas, hỗ trợ khối lượng cao;
- Kiểm chứng bằng chứng (Verification) cho sản phẩm, cơ quan và công dân;
- Thu hồi bằng chứng (Revocation) khi hồ sơ gốc bị thu hồi, hủy bỏ hoặc sửa đổi.

2.2. Kiến trúc cấu phần

Mô đun 2 gồm 05 hợp đồng thông minh trên DNC-Chain và bộ cấu phần off-chain chạy tại hạ tầng quản trị.

Bảng B.2.1. Hợp đồng thông minh của Mô đun 2

Hợp đồng	Chức năng
ProofRegistry	Sổ đăng ký bằng chứng trung tâm; ghi nhận hash kèm siêu dữ liệu (thời điểm, người ghi, loại bằng chứng, mã hồ sơ)
BatchManager	Quản lý gom giao dịch theo Merkle Tree; ghi Merkle Root của lô thay vì ghi từng bằng chứng
IssuerRegistry	Danh mục hệ thống nguồn được ủy quyền ghi bằng chứng và phạm vi loại bằng chứng mỗi hệ thống được phép tạo
RevocationList	Danh sách bằng chứng đã bị thu hồi; đánh dấu trạng thái kèm lý do, không xóa bản ghi gốc
VerificationLog	Nhật ký phiên kiểm chứng (ai kiểm, thời điểm, kết quả)

Cấu phần off-chain gồm Hash Engine, Batching Engine, Timestamp Service, Receipt Service, Verification Service và Integration SDK (thư viện tích hợp cho Java, Node.js, Python, .NET phục vụ các sản phẩm kết nối).

Mỗi bằng chứng lưu trên ProofRegistry gồm 08 trường: proofId (định danh duy nhất), docHash (hash nội dung hồ sơ), docType (loại hồ sơ), issuerDID (định danh hệ thống nguồn), subjectRef (tham chiếu đối tượng - Hub ID hoặc mã hồ sơ), timestamp, metadataURI (không chứa dữ liệu cá nhân), signature.

2.3. Quan hệ với các mô đun khác

Mô đun 2 gọi Mô đun 1 khi cần chia sẻ bằng chứng với chuỗi ngoài (ví dụ đối soát liên tỉnh qua VBSN). Mô đun 2 sử dụng RBAC của Mô đun 3 để xác định hệ thống nguồn được phép ghi, sản phẩm được phép kiểm chứng, cơ quan có quyền thu hồi. Các hợp đồng của Mô đun 2 được Mô đun 5 quản lý vòng đời. Khi bằng chứng liên quan đến người dùng, Mô đun 2 sử dụng Hub ID do Mô đun 7 cấp thay vì thông tin cá nhân.

2.4. Giao diện kỹ thuật chính

Mô đun 2 cung cấp ba nhóm giao diện tương ứng ba đối tượng tương tác:

Bảng B.2.2. Giao diện chính của Mô đun 2

Đối tượng	Nhóm giao diện	Chuẩn xác minh
Hệ thống nguồn qua LGSP	API nạp dữ liệu; API thu hồi	mTLS + JWT + chữ ký số ERC-191 của hệ thống nguồn
Sản phẩm ứng dụng SP1 - SP10	SDK tích hợp (Java, Node.js, Python, .NET); API kiểm chứng	JWT + chữ ký số của sản phẩm
Bên kiểm chứng độc lập (công dân, cơ quan, tổ chức)	Portal xác minh công khai; API kiểm chứng mở	Không bắt buộc với bằng chứng công khai; API key + rate limit với API kiểm chứng mở

Chuẩn dữ liệu đầu vào tuân thủ Khung kiến trúc dữ liệu quốc gia, định dạng JSON-LD hoặc W3C Verifiable Credentials Data Model **v2.0**; chuẩn siêu dữ liệu theo Dublin Core và các chuẩn chuyên ngành (HL7 FHIR cho hồ sơ y tế, European Learning Model cho văn bằng). Thuật toán băm: SHA-256 cho nội dung hồ sơ, keccak256 cho định danh bằng chứng (tương thích EVM).

2.5. Ràng buộc tuân thủ pháp lý

Mô đun 2 tuân thủ:

- Luật Giao dịch điện tử số 20/2023/QH15 (tính pháp lý của chữ ký số và dấu thời gian);

- Luật Dữ liệu số 60/2024/QH15 và Nghị định số 278/2025/NĐ-CP (kết nối qua LGSP theo chuẩn chung);

- Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP (không ghi dữ liệu cá nhân lên chuỗi; quyền xóa dữ liệu thực hiện qua thu hồi bằng chứng trên RevocationList);

- Luật Tiếp cận thông tin (công bố định kỳ số liệu thống kê vận hành, danh mục hệ thống nguồn được ủy quyền).

2.6. Cơ chế nâng cấp

Các hợp đồng của Mô đun 2 áp dụng Proxy Upgrade Pattern. Việc thêm, xóa hệ thống nguồn khỏi IssuerRegistry, thay đổi phạm vi ủy quyền của hệ thống nguồn, nâng cấp hợp đồng đều yêu cầu đa ký 2/3 của các cơ quan quản trị và timelock 48 giờ. Mọi thay đổi ghi vào VerificationLog bất biến.

2.7. Chỉ tiêu mức dịch vụ cốt lõi

Bảng B.2.3. Chỉ tiêu mức dịch vụ của Mô đun 2

Chỉ tiêu	Mục tiêu
Thời gian sẵn sàng	$\geq 99,9\%$ hàng tháng (mô đun cốt lõi, yêu cầu uptime cao)
Thời gian ghi bằng chứng đơn lẻ	≤ 30 giây từ khi nhận yêu cầu đến khi có biên lai
Thời gian ghi theo batch (≤ 1.000 bằng chứng)	≤ 60 giây
Thông lượng ghi tối đa qua batching	≥ 1.000 bằng chứng/giây
Tỷ lệ ghi thành công	$\geq 99,95\%$

2.8. Điều kiện triển khai

- Kết nối kỹ thuật với LGSP đã được thiết lập và nghiệm thu theo Nghị định số 278/2025/NĐ-CP;

- Các hệ thống nguồn tham gia đã đăng ký vào IssuerRegistry, có chữ ký số hợp lệ và phạm vi ủy quyền được phê duyệt;

- Kiểm toán bảo mật mã nguồn hợp đồng thông minh hoàn tất trước khi vận hành;

- Cơ chế đối soát định kỳ giữa nhật ký on-chain và hệ thống nghiệp vụ đã được thiết lập;

- Giai đoạn 2026 - 2027 ưu tiên phục vụ các sản phẩm Tầng 1 (SP1, SP2) theo Chương IV Mục II điểm 4 của Đề án; giai đoạn 2028 - 2030 mở rộng cho các sản phẩm có dữ liệu phức tạp và yêu cầu đối soát cao hơn.

Mô đun 3 - Quản lý khoá và phân quyền

3.1. Vai trò và chức năng chính

Mô đun 3 là mô đun nền tảng về an toàn của DNC-Chain, quản lý vòng đời khoá mật mã, định danh kỹ thuật và phân quyền truy cập cho toàn bộ chủ thể tham gia hệ sinh thái (tổ chức, cá nhân, hệ thống, ứng dụng, tiến trình tự động). Mô đun 3 đóng vai trò "lớp an toàn ngang" - tất cả các mô đun khác và toàn bộ sản phẩm phải sử dụng Mô đun 3 để xác minh, phân quyền và quản lý khoá.

Mô đun 3 không phải dịch vụ xác minh cuối người dùng của từng sản phẩm. Mô đun cung cấp cơ chế nền để các sản phẩm xây dựng dịch vụ xác minh phía trên, bảo đảm nguyên tắc "rõ quyền, rõ trách nhiệm, có căn cứ kiểm toán" được áp dụng thống nhất.

Năm chức năng kỹ thuật chính:

- Quản lý vòng đời khoá mật mã (tạo, đăng ký, luân phiên, sao lưu, thu hồi) qua Hardware Security Mô đun;
- Quản lý phân quyền theo cơ chế RBAC bốn lớp (mạng, tổ chức, ứng dụng, dịch vụ);
- Xác minh chủ thể tham gia, bao gồm tích hợp với Hệ thống định danh điện tử quốc gia VNeID qua OpenID Connect;
- Cấp và quản lý chứng thư số cho các node, tổ chức và hệ thống tham gia;
- Ghi nhận nhật ký bất biến mọi thay đổi phân quyền, cấp khoá, thu hồi phục vụ giám sát và hậu kiểm.

3.2. Kiến trúc cấu phần

Mô đun 3 gồm 05 hợp đồng thông minh và bộ cấu phần off-chain tích hợp với HSM và VNeID.

Bảng B.3.1. Hợp đồng thông minh của Mô đun 3

Hợp đồng	Chức năng
AccessControlRegistry	Sổ đăng ký phân quyền trung tâm; ánh xạ giữa định danh và vai trò; cơ chế RBAC bốn lớp
RoleManagement	Định nghĩa vai trò và quyền hạn; quản lý kế thừa vai trò giữa các lớp
KeyRegistry	Sổ đăng ký khóa công khai; ánh xạ DID - public key; trạng thái khóa (active, rotating, revoked)

Hợp đồng	Chức năng
RevocationList	Danh sách khoá và vai trò bị thu hồi; cập nhật thời gian thực
AuditLog	Nhật ký bất biến mọi thay đổi phân quyền, cấp khoá, thu hồi

Các chuẩn tuân thủ: OpenZeppelin AccessControl và ERC-165 cho phân quyền, W3C DID Core và ERC-1056 cho định danh phi tập trung, RFC 5280 (CRL compatible) cho danh sách thu hồi, EIP-712 cho nhật ký có cấu trúc.

Cấu phần off-chain gồm: Key Management Service (KMS) kết nối HSM qua chuẩn PKCS#11; RBAC Engine; Identity Gateway tích hợp VNeID qua OpenID Connect; OAuth 2.0 / OpenID Connect Provider phục vụ xác minh tổ chức và hệ thống; Audit Aggregator tổng hợp nhật ký giám sát.

RBAC bốn lớp cụ thể hoá nguyên lý nêu tại Phần A Mục VII điểm 1: vai trò mạng (ROLE_VALIDATOR, ROLE_RELAYER, ROLE_NETWORK_ADMIN - do Ủy ban nhân dân thành phố phê duyệt, thay đổi yêu cầu đa ký 3/5); vai trò tổ chức (ROLE_ORG_ADMIN, ROLE_ORG_OPERATOR, ROLE_ORG_AUDITOR); vai trò ứng dụng (định nghĩa riêng từng sản phẩm, kế thừa từ vai trò tổ chức); vai trò dịch vụ (ROLE_SERVICE_READER, ROLE_SERVICE_WRITER, ROLE_SERVICE_ADMIN - áp dụng cho API client và tiến trình tự động theo nguyên tắc đặc quyền tối thiểu).

3.3. Quan hệ với các mô đun khác

Mô đun 3 là nền tảng cho tất cả mô đun và sản phẩm khác. Quan hệ với Mô đun 7 có tính một chiều: Mô đun 7 sử dụng Mô đun 3 để cấp khoá cho Hub ID, nhưng Mô đun 3 không xử lý dữ liệu cá nhân. Quan hệ với Mô đun 5 có tính đối ứng: Mô đun 3 cấp quyền triển khai hợp đồng cho các bên, đồng thời các hợp đồng của Mô đun 3 được Mô đun 5 kiểm toán và quản lý phiên bản.

3.4. Giao diện kỹ thuật chính

Bảng B.3.2. Giao diện chính của Mô đun 3

Nhóm giao diện	Giao thức	Chuẩn xác minh
Quản lý khoá (KMS API)	gRPC + mTLS	mTLS + JWT quản trị + đa ký với thao tác quan trọng
Phân quyền (RBAC API)	REST	JWT + chữ ký số
Xác minh công dân (Identity Gateway)	OpenID Connect qua VNeID	OIDC Authorization Code Flow + PKCE

Nhóm giao diện	Giao thức	Chuẩn xác minh
Xác minh tổ chức và hệ thống (OAuth 2.0 Provider)	OAuth 2.0	Client Credentials Grant + mTLS
Giám sát và kiểm toán (Audit API)	REST + WebSocket	JWT + quyền ROLE_AUDITOR

Kết nối với HSM tuân thủ chuẩn PKCS#11. HSM sử dụng theo yêu cầu tại Phần A Mục VII điểm 3: ưu tiên thiết bị do doanh nghiệp, tổ chức Việt Nam sản xuất đã được Ban Cơ yếu Chính phủ chứng nhận đạt quy chuẩn tương đương FIPS 140-3 Level 3.

Tích hợp với VNeID qua OpenID Connect Authorization Code Flow với PKCE, phạm vi yêu cầu giới hạn ở openid + profile + vneid_level (không yêu cầu scope chứa thông tin cá nhân chi tiết). Mô đun 3 chỉ nhận "mức xác minh VNeID" (Mức 1 hoặc Mức 2 theo Nghị định số 69/2024/NĐ-CP) và định danh tham chiếu từ VNeID; không lưu trữ thông tin cá nhân; không thay thế VNeID trong vai trò định danh gốc.

3.5. Ràng buộc tuân thủ pháp lý

Mô đun 3 tuân thủ:

- Luật Giao dịch điện tử số 20/2023/QH15 và quy chuẩn mật mã dân sự của Ban Cơ yếu Chính phủ (thuật toán mật mã được phép sử dụng; chuẩn HSM);
- Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP (tích hợp VNeID không lưu thông tin cá nhân; nhật ký truy vấn phục vụ quyền chủ thể dữ liệu);
- Luật An toàn thông tin mạng số 86/2015/QH13 (được sửa đổi, bổ sung bởi Luật số 35/2018/QH14) và Luật An ninh mạng số 24/2018/QH14, được hợp nhất và thay thế bởi Luật An ninh mạng số 116/2025/QH15 kể từ ngày 01/7/2026 (nhật ký bất biến; phân cấp bảo mật hệ thống);
- Các quy định của Bộ Công an về tích hợp với VNeID.

3.6. Cơ chế nâng cấp

Áp dụng Proxy Upgrade Pattern cho tất cả hợp đồng. Nâng cấp hợp đồng, thay đổi định nghĩa vai trò cấp mạng, thay đổi cấu hình HSM đều yêu cầu đa ký 3/5 của quản trị viên được ủy quyền và timelock 48 giờ. Thay đổi vai trò cấp tổ chức và cấp ứng dụng theo cơ chế đa ký nhẹ hơn do từng cơ quan chủ trì quyết định. Toàn bộ thay đổi ghi vào AuditLog bất biến.

3.7. Chỉ tiêu mức dịch vụ cốt lõi

Bảng B.3.3. Chỉ tiêu mức dịch vụ của Mô đun 3

Chỉ tiêu	Mục tiêu
----------	----------

Chỉ tiêu	Mục tiêu
Thời gian sẵn sàng	$\geq 99,99\%$ hàng tháng (yêu cầu uptime cao nhất trong 07 mô đun)
Thời gian phản hồi kiểm tra quyền (hasRole)	≤ 100 mili-giây
Thời gian cấp khóa mới	≤ 2 phút (gồm tạo khóa trong HSM, đăng ký on-chain, phát hành chứng thư)
Thời gian thu hồi khẩn cấp	≤ 1 phút từ khi phê duyệt đến khi toàn mạng cập nhật
Tỷ lệ ghi nhật ký đầy đủ các yêu cầu truy cập trái phép	100%

3.8. Điều kiện triển khai

- Hệ thống HSM đã được lắp đặt và vận hành tại tối thiểu 03 cơ sở nhà nước độc lập với cấu hình active-active;
- Thiết bị HSM đã được Ban Cơ yếu Chính phủ kiểm định và chứng nhận;
- Kết nối kỹ thuật với VNeID đã được Bộ Công an chấp thuận và nghiệm thu;
- Quy trình key ceremony đã được ban hành và diễn tập với đại diện các cơ quan liên quan;
- Kiểm định mật mã bởi đơn vị được Ban Cơ yếu Chính phủ chỉ định đã hoàn tất trước khi vận hành chính thức;

Giai đoạn 2026 - 2027 triển khai đồng bộ với hạ tầng DNC-Chain và các mô đun nền tảng khác; giai đoạn 2028 - 2030 hoàn thiện, mở rộng theo nhu cầu phát triển ứng dụng.

Mô đun 4 - Quản lý giao dịch và Token

4.1. Vai trò và chức năng chính

Mô đun 4 là mô đun quản lý đơn vị ghi nhận số (token nội bộ) và trạng thái giao dịch trên DNC-Chain, phục vụ các chức năng nghiệp vụ, quản trị, xác minh, chứng nhận, điểm thưởng và các trường hợp được phép trong phạm vi Đề án. Mô đun 4 bám sát ràng buộc bắt buộc tại Chương III Mục II và Chương IV Mục II điểm 4 của Đề án: không hình thành cơ chế giao dịch tài sản mã hoá công khai trên hạ tầng dùng chung.

Tính chất định vị này có ba hệ quả kỹ thuật quan trọng:

- DNC-Chain không triển khai sản giao dịch tài sản mã hoá; không tổ chức thị trường trao đổi token với giá biến động theo cung cầu; không có cơ chế tạo lập thị trường tự động.

- Mô đun 4 sử dụng các chuẩn kỹ thuật token (ERC-20, ERC-721, ERC-1155) do yêu cầu tương thích EVM, nhưng các token phát hành chỉ là đơn vị ghi nhận số phục vụ nghiệp vụ, không phải tài sản mã hoá công khai;

- Các ứng dụng có yếu tố giao dịch tài sản mã hoá thực sự (SP8, SP9, SP10 thuộc Tầng 4) triển khai theo cơ chế riêng gắn với **IFC**, **không sử dụng Mô đun 4** của hạ tầng dùng chung cho chức năng này.

Năm chức năng kỹ thuật chính:

- Phát hành token theo các chuẩn (Platform Utility, Soulbound, Transferable có kiểm soát, Loyalty, Governance);

- Quản lý vòng đời giao dịch token (chuyển nhượng, đốt, khoá);

- Thực thi quy tắc tuân thủ tự động tại lớp hợp đồng thông minh qua Compliance Layer;

- Duy trì sổ cái token và lịch sử giao dịch phục vụ đối soát, kiểm toán, truy vết;

- Cổng chuyển đổi có kiểm soát (ConversionGateway) phục vụ các trường hợp đặc biệt được phê duyệt.

4.2. Kiến trúc cấu phần và phân loại token

Mô đun 4 gồm 06 hợp đồng thông minh:

Bảng B.4.1. Hợp đồng thông minh của Mô đun 4

Hợp đồng	Chức năng
TokenFactory	Nhà máy phát hành token theo template chuẩn; cấu hình tổng cung, khả năng chuyển nhượng, thời hạn
TokenRegistry	Sổ đăng ký toàn bộ token đã phát hành; thông tin đơn vị phát hành, cấu hình, trạng thái
ComplianceEngine	Lớp tuân thủ trung tâm; thực thi quy tắc giới hạn trước khi cho phép giao dịch
TransactionManager	Quản lý vòng đời giao dịch; kiểm tra điều kiện tiên quyết; hỗ trợ batch
TokenLedger	Sổ cái token; lịch sử số dư và giao dịch; hỗ trợ truy vết nhiều chiều

Hợp đồng	Chức năng
ConversionGateway	Cửa ngõ chuyển đổi có kiểm soát giữa token nội bộ và các đơn vị khác khi được phép

Các chuẩn tuân thủ: ERC-20 (token có thể thay thế), ERC-721 (token không thể thay thế), ERC-1155 (token đa tiêu chuẩn), EIP-1400 (security token với Compliance).

Phân loại token trong hệ sinh thái DNC-Chain:

Bảng B.4.2. Phân loại token trên DNC-Chain

Nhóm token	Mục đích	Khả năng chuyển nhượng	Ví dụ
Token tiện ích nền tảng (Platform Utility)	Đo lường và tính phí giao dịch nội bộ	Không giao dịch tự do; chỉ sử dụng nội bộ	Token gas của DNC-Chain
Token không thể chuyển nhượng (Soulbound - SBT)	Gắn với danh tính chủ thể	Không chuyển nhượng được	Token văn bằng SP2, token chứng chỉ hành nghề
Token có thể chuyển nhượng có kiểm soát	Đại diện quyền sở hữu hoặc sử dụng tài sản	Chuyển nhượng có điều kiện theo Compliance	Token sở hữu trí tuệ SP6
Token điểm thưởng (Loyalty)	Ghi nhận điểm thưởng thành phố	Chuyển nhượng trong phạm vi hẹp theo quy tắc	DaNang Point - SP7
Token quản trị (Governance)	Bỏ phiếu quyết định quản trị nội bộ	Không chuyển nhượng; cấp có kiểm soát	Token bỏ phiếu validator

4.3. Quan hệ với các mô đun khác

Mô đun 4 sử dụng Mô đun 2 để ghi bằng chứng xác minh đối với các giao dịch token quan trọng (phát hành, chuyển nhượng giá trị lớn). Sử dụng RBAC của Mô đun 3 để kiểm soát quyền phát hành, chuyển nhượng, quản trị Compliance. Các hợp đồng token tuân thủ thư viện mẫu đã được Mô đun 5 kiểm toán; mọi token mới phải qua quy trình phê duyệt của Mô đun 5. Các giao dịch của người dùng sử dụng Hub ID do Mô đun 7 cấp thay vì thông tin cá nhân.

4.4. Giao diện kỹ thuật chính

Bảng B.4.3. Giao diện chính của Mô đun 4

Nhóm giao diện	Chức năng	Chuẩn xác minh
Phát hành token	Tạo token mới, cấu hình tham số, cập nhật metadata	JWT + đa ký của đơn vị được ủy quyền
Giao dịch token	Chuyển nhượng, đốt, khoá, kiểm tra số dư	JWT + chữ ký số của chủ sở hữu
Compliance API	Cấu hình quy tắc tuân thủ; truy vấn trạng thái	JWT + ROLE_COMPLIANCE_ADMIN
Ledger API	Truy vấn số dư, lịch sử giao dịch, truy vết	JWT (tùy theo quyền)
Conversion API	Gửi và phê duyệt yêu cầu chuyển đổi	JWT + đa ký của cơ quan chức năng

Compliance Layer là thành phần đặc thù của Mô đun 4, thực thi các quy tắc tuân thủ tự động tại lớp hợp đồng thông minh trước khi giao dịch được ghi lên chuỗi. Các loại quy tắc gồm: giới hạn số dư tối đa (Balance Cap); hạn chế đối tượng nắm giữ theo VC (Holder Restriction); yêu cầu mức xác minh VNeID để nhận token giá trị lớn (KYC Gate); hạn chế chuyển nhượng theo danh sách cho phép (Transfer Restriction); khoá theo thời gian (Time-lock); thời hạn hiệu lực (Expiry). Nếu không thỏa mãn, giao dịch bị từ chối; cơ chế này bảo đảm tính tuân thủ ngay cả khi nhiều ứng dụng cùng tương tác với một loại token.

4.5. Ràng buộc tuân thủ pháp lý và giới hạn phạm vi tuyệt đối

Mô đun 4 tuân thủ Luật Giao dịch điện tử, Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân và các quy định chuyên ngành (chứng khoán, thị trường vốn, phòng chống rửa tiền, phòng chống tài trợ khủng bố nếu áp dụng đối với các mô hình Tầng 4 theo cơ chế riêng).

Mô đun 4 được thiết kế với các ràng buộc kỹ thuật tuyệt đối, không thể vượt qua, bảo đảm không phát sinh chức năng giao dịch tài sản mã hóa công khai:

- Không có cơ chế tạo lập thị trường tự động (automated market maker) trong bất kỳ hợp đồng nào;
- Không có orderbook hoặc cơ chế khớp lệnh; mọi chuyển nhượng là điểm tới điểm có kiểm soát;

- Không có cơ chế staking để người dùng khoá token và nhận thưởng theo mô hình tài chính phi tập trung;

- Không có cầu nối hai chiều tự do sang các mạng công khai (Mô đun 1 chỉ truyền thông điệp, không chuyển giao tài sản);

- Mọi token phát hành mới phải qua quy trình phê duyệt; không có cơ chế tự phát hành không kiểm soát.

Các ràng buộc này được cài đặt ở cấp mã nguồn của hợp đồng thông minh và chỉ có thể điều chỉnh qua cơ chế nâng cấp tại Mục 4.6 dưới đây, với sự phê duyệt của Ủy ban nhân dân thành phố.

4.6. Cơ chế nâng cấp

Hợp đồng của Mô đun 4 áp dụng Proxy Upgrade Pattern. Việc phát hành loại token mới, nâng cấp hợp đồng cốt lõi (TokenFactory, ComplianceEngine), thay đổi quy tắc Compliance cấp hệ thống đều yêu cầu đa ký 3/5 và timelock 48 giờ, phải có kiểm toán bảo mật mã nguồn của hợp đồng mới hoàn tất trước khi thực thi thay đổi. Việc điều chỉnh các ràng buộc kỹ thuật tuyệt đối tại Mục 4.5 (nếu có) yêu cầu phê duyệt của Ủy ban nhân dân thành phố.

4.7. Chỉ tiêu mức dịch vụ cốt lõi

Bảng B.4.4. Chỉ tiêu mức dịch vụ của Mô đun 4

Chỉ tiêu	Mục tiêu
Thời gian sẵn sàng	≥ 99,9% hàng tháng
Thời gian phát hành token cho người dùng	≤ 10 giây (bao gồm kiểm tra Compliance và ghi on-chain)
Thời gian chuyển nhượng token	≤ 5 giây
Thông lượng giao dịch token	≥ 500 giao dịch/giây
Tỷ lệ đối soát thành công giữa sổ cái on-chain và hệ thống off-chain	100% tại mỗi chu kỳ đối soát hàng ngày

4.8. Điều kiện triển khai

- Thư viện hợp đồng mẫu (template) cho từng loại token đã được Mô đun 5 kiểm toán và phê duyệt;

- Cấu hình Compliance cho từng loại token đã được xác định và ban hành bằng văn bản;

- Cơ chế đối soát định kỳ giữa sổ cái on-chain và hệ thống nghiệp vụ các sản phẩm đã được thiết lập;

- Đối với ConversionGateway: chỉ vận hành khi Ủy ban nhân dân thành phố đã phê duyệt cụ thể từng trường hợp ứng dụng Tầng 4 (SP8); Mô đun 4 không thực hiện chuyển đổi tự động, chỉ cung cấp thành phần kỹ thuật phục vụ quy trình đã được phê duyệt;

- Giai đoạn 2026 - 2027 ưu tiên xây dựng các chức năng phục vụ các sản phẩm triển khai sớm (SP2); giai đoạn 2028 - 2030 mở rộng cho các sản phẩm Tầng 3 (SP6) và hỗ trợ kỹ thuật cho Tầng 4 theo phạm vi được phép.

Mô đun 5 - Quản lý smart contract

5.1. Vai trò và chức năng chính

Mô đun 5 là mô đun quản trị vòng đời hợp đồng thông minh trên DNC-Chain, bao gồm phát triển, kiểm thử, kiểm toán, phê duyệt, triển khai, nâng cấp và loại bỏ. Mô đun đóng vai trò "trung tâm điều phối thay đổi" của hạ tầng: mọi hợp đồng thông minh đều phải qua Mô đun 5 trước khi triển khai chính thức, và mọi nâng cấp sau này cũng phải qua Mô đun 5.

Vai trò này khiến Mô đun 5 trở thành cơ sở hạ tầng kỹ thuật cho tính mở và khả năng tiến hoá của DNC-Chain. Nhờ Mô đun 5, các mô đun khác có thể cập nhật logic nghiệp vụ, bổ sung chuẩn mới (ví dụ từ ERC-721 sang ERC-1400 cho token tuân thủ) hoặc thay thế thuật toán mật mã (khi chuyển sang mật mã hậu lượng tử theo Phần A Mục VII điểm 4) mà không phá vỡ kiến trúc tổng thể. Mô đun 5 bảo đảm nguyên tắc nêu tại Chương IV Mục II điểm 4 của Đề án: Mô đun có thể được nâng cấp, thay thế hoặc mở rộng theo từng giai đoạn triển khai mà không làm thay đổi kiến trúc lõi.

Năm chức năng kỹ thuật chính:

- Đăng ký và quản lý danh mục hợp đồng thông minh trên toàn bộ DNC-Chain;
- Quản trị quy trình nâng cấp hợp đồng qua Proxy Upgrade Pattern với đa ký và timelock;
- Cung cấp thư viện hợp đồng mẫu (TemplateLibrary) đã qua kiểm toán để các mô đun, sản phẩm phát triển nhanh và an toàn;
- Điều phối quy trình kiểm toán bảo mật mã nguồn hợp đồng thông minh;
- Ghi nhật ký bất biến mọi thay đổi hợp đồng (triển khai, nâng cấp, thu hồi, tạm dừng).

5.2. Kiến trúc cấu phần và thư viện hợp đồng mẫu

Mô đun 5 gồm 05 hợp đồng thông minh quản trị và bộ cấu phần off-chain hỗ trợ phát triển.

Bảng B.5.1. Hợp đồng thông minh của Mô đun 5

Hợp đồng	Chức năng
----------	-----------

Hợp đồng	Chức năng
ContractRegistry	Sổ đăng ký toàn bộ hợp đồng trên DNC-Chain; thông tin về địa chỉ, phiên bản, chủ sở hữu, trạng thái
ProxyAdmin	Quản trị các Proxy contract theo mẫu Transparent Proxy và UUPS Proxy; thực thi nâng cấp implementation
UpgradeGovernance	Quản lý quy trình phê duyệt nâng cấp; thực thi cơ chế đa ký và timelock
AuditTrail	Nhật ký bất biến mọi thay đổi hợp đồng
TemplateLibrary	Thư viện hợp đồng mẫu đã kiểm toán

Các chuẩn tuân thủ: EIP-1967 (Standard Proxy Storage Slots), EIP-1822 (UUPS Proxy), OpenZeppelin Transparent Proxy, OpenZeppelin TimelockController, ERC-165.

Cấu phần off-chain gồm Development Portal (cổng phát triển hợp đồng), CI/CD Pipeline (tích hợp và triển khai liên tục), Audit Dashboard và Simulation Environment (môi trường mô phỏng trước khi triển khai).

TemplateLibrary cung cấp các mẫu hợp đồng đã qua kiểm toán bảo mật, sẵn sàng triển khai.

Bảng B.5.2. Thư viện hợp đồng mẫu ban đầu của DNC-Chain

Mẫu	Chuẩn tuân thủ	Mô đun / sản phẩm sử dụng
ProofRegistryTemplate (ghi và truy xuất bằng chứng mật mã)	EIP-712	Mô đun 2, SP1, SP2, SP4, SP6
TokenStandardTemplate (phát hành token)	ERC-20, ERC-721, ERC-1155	Mô đun 4, SP2, SP5, SP6, SP7
AccessControlTemplate (RBAC trên chuỗi)	OpenZeppelin AccessControl	Mô đun 3, toàn bộ sản phẩm

Mẫu	Chuẩn tuân thủ	Mô đun / sản phẩm sử dụng
EscrowTemplate (ký quỹ thông minh cho giao dịch có điều kiện)	-	SP6, có thể mở rộng
MultiSignatureTemplate (phê duyệt đa bên)	Gnosis Safe compatible	Toàn bộ mô đun cần đa ký
GovernanceTemplate (bỏ phiếu và thực thi quản trị)	OpenZeppelin Governor	Quản trị DNC-Chain
OracleInterfaceTemplate (giao diện chuẩn hoá nhận dữ liệu ngoài chuỗi)	AggregatorV3Interface (tương thích chuẩn, không phụ thuộc dịch vụ Chainlink thương mại)	SP3, SP5

Thư viện không cố định. Khi có chuẩn mới phát sinh (ERC-4626 cho vault token, ERC-6551 cho token-bound accounts, các chuẩn hậu lượng tử khi ban hành), cơ quan quản trị có thể bổ sung mẫu mới. Các mẫu cũ nếu không còn phù hợp chuyển sang trạng thái "deprecated" (không khuyến cáo sử dụng) nhưng vẫn được hỗ trợ để các hợp đồng đã triển khai trước đó tiếp tục vận hành.

5.3. Quan hệ với các mô đun khác

Mô đun 5 có quan hệ hai chiều đặc biệt với Mô đun 3: Mô đun 3 cấp quyền triển khai hợp đồng cho các bên được ủy quyền; đồng thời các hợp đồng của Mô đun 3 được Mô đun 5 quản lý vòng đời. Mô đun 5 có quan hệ một chiều với các mô đun 1, 2, 4, 6, 7 và toàn bộ 10 sản phẩm: tất cả hợp đồng thông minh của chúng đều do Mô đun 5 quản lý. Mô đun 5 không quản lý các câu phân off-chain; phần off-chain được quản lý bởi cơ quan vận hành hạ tầng theo quy trình DevOps chuẩn.

5.4. Giao diện kỹ thuật chính

Bảng B.5.3. Giao diện chính của Mô đun 5

Nhóm giao diện	Chức năng	Chuẩn xác minh
Phát triển (Development Portal)	Đăng ký hợp đồng mới, tải mã nguồn, yêu cầu kiểm toán	JWT + chữ ký số đơn vị phát triển
Triển khai (Deployment API)	Triển khai lên môi trường thử nghiệm, staging, production	JWT + ROLE_DEPLOYER

Nhóm giao diện	Chức năng	Chuẩn xác minh
Nâng cấp (Upgrade API)	Đề xuất nâng cấp, theo dõi phê duyệt, thực thi	JWT + đa ký của UpgradeGovernance
Kiểm toán (Audit API)	Truy vấn trạng thái kiểm toán, tải báo cáo, phản hồi	JWT + ROLE_AUDITOR
Giám sát (Monitoring API)	Truy vấn thông tin hợp đồng, đăng ký thông báo thay đổi	JWT (tùy theo quyền)

Mô đun 5 tích hợp với các công cụ phát triển Ethereum phổ biến để đội ngũ kỹ thuật có thể tự do lựa chọn: Hardhat, Foundry, Truffle (framework phát triển - có plugin tích hợp); Slither, Mythril, Echidna (công cụ phân tích tĩnh và fuzzing - tích hợp vào CI/CD Pipeline); Etherscan-compatible Explorer (trình duyệt khối tra cứu mã nguồn đã xác minh).

5.5. Ràng buộc tuân thủ pháp lý

Mô đun 5 tuân thủ quy định chung tại Phần A Mục XII về kiểm toán kỹ thuật (Technical Audit). Các hợp đồng thông minh cốt lõi của mọi mô đun và sản phẩm phải qua kiểm toán bảo mật độc lập bởi tổ chức kiểm toán đủ năng lực trước khi triển khai lên hạ tầng vận hành chính thức; kiểm toán lặp lại sau mỗi lần nâng cấp lớn. Việc công khai mã nguồn đã xác minh (verified source code) trên trình duyệt khối đáp ứng yêu cầu minh bạch theo Luật Tiếp cận thông tin.

5.6. Cơ chế nâng cấp

Mô đun 5 chính là mô đun cung cấp cơ chế nâng cấp cho toàn bộ DNC-Chain. Cơ chế nâng cấp áp dụng cho các hợp đồng của Mô đun 5 tuân thủ các ràng buộc nghiêm ngặt:

- Nâng cấp hợp đồng thông thường: timelock tối thiểu 48 giờ;
- Nâng cấp hợp đồng lõi (của Mô đun 5, Mô đun 3): timelock tối thiểu 07 ngày;
- Nâng cấp khẩn cấp (khi phát hiện lỗ hổng nghiêm trọng): có thể rút ngắn timelock xuống tối thiểu 06 giờ với sự phê duyệt đặc biệt của Ủy ban nhân dân thành phố.

Các ràng buộc này được cài đặt cứng tại UpgradeGovernance; không thể rút ngắn dưới ngưỡng trừ khi có quyết định của cấp có thẩm quyền. Hợp đồng trong quá trình nâng cấp có thể được tạm dừng khẩn cấp (pause) qua ProxyAdmin; gỡ tạm dừng yêu cầu đa ký và báo cáo khắc phục sự cố.

Mọi hợp đồng đều phải đạt các tiêu chí kỹ thuật tối thiểu trước khi triển khai: độ bao phủ kiểm thử đơn vị không dưới 90%; phân tích tĩnh không phát hiện cảnh báo nghiêm trọng chưa xử lý; chi phí gas các hàm chính nằm trong ngưỡng chấp nhận được; mã nguồn được xác minh trên trình duyệt khối.

5.7. Chỉ tiêu mức dịch vụ cốt lõi

Bảng B.5.4. Chỉ tiêu mức dịch vụ của Mô đun 5

Chỉ tiêu	Mục tiêu
Thời gian sẵn sàng	$\geq 99,9\%$ hàng tháng
Thời gian CI/CD Pipeline hoàn tất (phân tích tĩnh, kiểm thử, đo độ bao phủ)	≤ 30 phút
Thời gian triển khai hợp đồng lên môi trường	≤ 5 phút mỗi môi trường
Thời gian chờ thực thi (timelock) nâng cấp	≥ 48 giờ với hợp đồng thường; ≥ 7 ngày với hợp đồng lõi; ≥ 6 giờ với nâng cấp khẩn cấp có phê duyệt đặc biệt
Tỷ lệ hợp đồng triển khai thành công qua kiểm toán	100% (hợp đồng không đạt kiểm toán không được triển khai)

5.8. Điều kiện triển khai

- Thư viện hợp đồng mẫu ban đầu đã hoàn tất kiểm toán bảo mật;
- Quy trình kiểm toán đã được ban hành, đơn vị kiểm toán độc lập đã được chọn;
- Các môi trường (thử nghiệm, staging, production) đã được cấu hình và tách biệt;
- CI/CD Pipeline đã được thiết lập và tích hợp các công cụ phân tích tĩnh;
- Quy trình đa ký phê duyệt nâng cấp đã được xác lập bằng văn bản, các cơ quan quản trị đã đăng ký khóa đa ký;
- Mô đun 5 triển khai đồng thời với hạ tầng DNC-Chain ngay giai đoạn đầu 2026 vì là mô đun nền tảng phục vụ tất cả các mô đun khác và toàn bộ sản phẩm.

Mô đun 6 - Quản lý ứng dụng và marketplace

6.1. Vai trò và chức năng chính

Mô đun 6 là mô đun quản lý vòng đời ứng dụng trên DNC-Chain và hỗ trợ tra cứu, tích hợp, tái sử dụng các giải pháp đã được cấp phép. Trong khi Mô đun 5 quản lý hợp

đồng thông minh ở cấp độ kỹ thuật thấp, Mô đun 6 quản lý ứng dụng như một thực thể nghiệp vụ ở cấp độ cao (product hoặc application), gồm nhiều hợp đồng cùng phối hợp và các cấu phần off-chain đi kèm.

Mô đun 6 là cơ sở hạ tầng kỹ thuật trực tiếp hỗ trợ việc mở rộng danh mục sản phẩm của DNC-Chain. Khi cần bổ sung ứng dụng mới ngoài 10 sản phẩm ban đầu của Đề án hoặc mở rộng phạm vi của ứng dụng hiện có, toàn bộ quy trình tiếp nhận, thẩm định, thử nghiệm, vận hành đều qua Mô đun 6. Điều này bám sát định hướng tại Chương IV Mục I điểm 2 của Đề án về ban hành quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời đối với các ứng dụng kết nối với DNC-Chain, bảo đảm DNC-Chain có khả năng phát triển theo thời gian mà vẫn giữ được kỷ luật quản trị.

Năm chức năng kỹ thuật chính:

- Đăng ký ứng dụng mới và quản lý danh mục ứng dụng trên DNC-Chain;
- Quản lý trạng thái vòng đời ứng dụng (đề xuất → thử nghiệm → sandbox → vận hành chính thức → mở rộng → kết thúc);
- Kiểm soát truy cập cấp ứng dụng (AccessGate) khi có yêu cầu đặc thù;
- Theo dõi việc sử dụng ứng dụng phục vụ đánh giá và mở rộng;
- Công bố Marketplace công khai để các cơ quan, doanh nghiệp, người dân tra cứu và tái sử dụng giải pháp.

6.2. Kiến trúc cấu phần

Mô đun 6 gồm 05 hợp đồng thông minh và bộ cấu phần off-chain.

Bảng B.6.1. Hợp đồng thông minh của Mô đun 6

Hợp đồng	Chức năng
ApplicationRegistry	Sổ đăng ký toàn bộ ứng dụng; thông tin về tên, cơ quan chủ trì, mô tả, hợp đồng liên quan, trạng thái
LifecycleManager	Quản lý trạng thái vòng đời 6 giai đoạn
AccessGate	Cổng kiểm soát truy cập cấp ứng dụng; điều phối quyền truy cập giữa người dùng và ứng dụng
UsageTracker	Theo dõi số lượng giao dịch, số người dùng, tần suất sử dụng
MarketplaceCatalog	Danh mục công khai; hỗ trợ tìm kiếm, phân loại, xếp hạng

Cấu phần off-chain gồm Marketplace Portal (giao diện công khai), Application Registration Service, Usage Analytics Engine, Developer Hub (công hỗ trợ đội phát triển).

Marketplace Portal là cổng công khai nơi các cơ quan, doanh nghiệp, người dân có thể tra cứu các ứng dụng đang vận hành trên DNC-Chain. Portal cung cấp: duyệt ứng dụng theo lĩnh vực (giáo dục, y tế, hành chính, kinh tế...); thông tin chi tiết (cơ quan chủ trì, giai đoạn, thống kê sử dụng, tài liệu hướng dẫn); liên kết đến giao diện sử dụng. Portal không chỉ là danh bạ tĩnh mà là công cụ thúc đẩy tái sử dụng - các cơ quan có thể tìm ra giải pháp đã có thay vì phát triển mới, tiết kiệm chi phí và thời gian.

6.3. Quan hệ với các mô đun khác

Mô đun 6 tương tác với toàn bộ các mô đun khác theo chiều đặc biệt: Mô đun 6 là điểm tiếp nhận đầu vào (đăng ký ứng dụng mới) và điểm xuất bản đầu ra (Marketplace công khai); các mô đun còn lại cung cấp dịch vụ cho ứng dụng qua Mô đun 6 làm trung gian quản trị. Cụ thể: quan hệ với Mô đun 3 về phân quyền truy cập; với Mô đun 5 về quản lý hợp đồng thông minh của ứng dụng; với Mô đun 2 về ghi bằng chứng hoạt động quan trọng của ứng dụng.

6.4. Giao diện kỹ thuật chính

Bảng B.6.2. Giao diện chính của Mô đun 6

Nhóm giao diện	Chức năng	Chuẩn xác minh
Đăng ký ứng dụng (Registration API)	Đề xuất ứng dụng mới, tải tài liệu kỹ thuật và nghiệp vụ	JWT + chữ ký số của cơ quan đề xuất
Quản lý vòng đời (Lifecycle API)	Chuyển trạng thái ứng dụng theo từng giai đoạn	JWT + ROLE_LIFECYCLE_ADMIN
Tra cứu công khai (Public Catalog API)	Tra cứu ứng dụng, mô tả, thống kê sử dụng công khai	Không bắt buộc
Truy cập ứng dụng (Access API)	Người dùng xin quyền sử dụng; ứng dụng gọi các mô đun khác	JWT + Hub ID
Giám sát sử dụng (Analytics API)	Truy vấn thống kê sử dụng theo nhiều chiều	JWT + quyền tương ứng
Hỗ trợ phát triển (Developer Hub API)	Truy cập tài liệu, SDK, môi trường thử nghiệm	JWT của đơn vị phát triển

Mô đun 6 hoạt động ở tầng quản trị, không nằm trên đường truy cập người dùng. AccessGate chỉ được gọi khi ứng dụng có yêu cầu kiểm soát truy cập ở cấp ứng dụng (ví dụ: chỉ cho phép công dân có VC Level 2 trở lên sử dụng một số chức năng nhất định).

6.5. Ràng buộc tuân thủ pháp lý

Mô đun 6 bám sát quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời ứng dụng do Sở Khoa học và Công nghệ ban hành theo yêu cầu tại Chương IV Mục I điểm 2 của Đề án. Kết quả đánh giá định kỳ từng ứng dụng được công bố trên Marketplace Portal theo Luật Tiếp cận thông tin. Việc đưa ứng dụng mới ra ngoài 10 sản phẩm của Đề án yêu cầu phê duyệt của Ủy ban nhân dân thành phố; mở rộng phạm vi ứng dụng hiện có do Sở Khoa học và Công nghệ phê duyệt.

6.6. Cơ chế nâng cấp

Các hợp đồng của Mô đun 6 áp dụng Proxy Upgrade Pattern qua Mô đun 5. Khi ứng dụng nâng cấp phiên bản, Mô đun 6 phối hợp với Mô đun 5: Mô đun 5 quản lý nâng cấp hợp đồng thông minh của ứng dụng; Mô đun 6 quản lý metadata (mô tả mới, tài liệu mới, thông báo cho người dùng). Việc chuyển trạng thái vòng đời ứng dụng (ví dụ từ thử nghiệm sang vận hành chính thức) yêu cầu phê duyệt theo thẩm quyền đã nêu tại Mục 6.5.

6.7. Chỉ tiêu mức dịch vụ cốt lõi

Bảng B.6.3. Chỉ tiêu mức dịch vụ của Mô đun 6

Chỉ tiêu	Mục tiêu
Thời gian sẵn sàng	$\geq 99,5\%$ hàng tháng
Thời gian phản hồi Marketplace Portal (tải thường)	≤ 2 giây
Thời gian phản hồi dưới tải đỉnh (10.000 người dùng đồng thời)	≤ 3 giây
Thời gian xử lý đăng ký ứng dụng (tự động, không bao gồm thời gian thẩm định nghiệp vụ)	≤ 5 phút
Sức chứa Marketplace	Không giới hạn kỹ thuật về số ứng dụng (kiến trúc phẳng của ApplicationRegistry)

Mô đun 6 được thiết kế để hỗ trợ tiếp nhận hàng chục đến hàng trăm ứng dụng trong các giai đoạn tiếp theo khi DNC-Chain trở thành hạ tầng dùng chung thực sự của thành phố, vượt xa danh mục 10 sản phẩm ban đầu của Đề án.

6.8. Điều kiện triển khai

- Quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời ứng dụng do Sở Khoa học và Công nghệ ban hành đã có hiệu lực;
- Các tiêu chí kỹ thuật, tiêu chí đánh giá định kỳ đã được xác lập;
- Marketplace Portal đã sẵn sàng về giao diện và nội dung;
- Giai đoạn 2026 - 2027 ưu tiên đăng ký, tích hợp và giám sát các sản phẩm trọng tâm (SP1, SP2); giai đoạn 2028 - 2030 mở rộng kho ứng dụng, cơ chế tái sử dụng và tiếp nhận các ứng dụng ngoài danh mục ban đầu.

Mô đun 7 - Hub làm sạch dữ liệu

7.1. Vai trò và chức năng chính

Mô đun 7 là mô đun kỹ thuật bảo đảm hai yêu cầu đồng thời: xác minh được danh tính chủ thể đứng sau giao dịch phục vụ quản lý, kiểm toán, truy vết khi có yêu cầu pháp lý hợp lệ; và không ghi thông tin nhận dạng cá nhân lên sổ cái blockchain, tuân thủ nguyên tắc thu thập tối thiểu theo Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP.

Mô đun 7 thực hiện điều này qua mô hình "cổng kiểm soát hai chiều". Ở cổng vào, Mô đun 7 tiếp nhận kết quả xác minh từ hệ thống nguồn (qua VNeID đối với công dân, qua chứng thư doanh nghiệp đối với tổ chức, qua chữ ký số cơ quan) và cấp mã định danh kỹ thuật vô danh (Hub ID) kèm Chứng nhận xác minh (VC). Ở cổng ra, khi có yêu cầu pháp lý hợp lệ, Mô đun 7 hỗ trợ cơ quan có thẩm quyền truy ngược từ Hub ID về chủ thể thực; tuy nhiên việc tra cứu cụ thể thực hiện tại hệ thống nguồn, không tại Mô đun 7.

Mô đun 7 không thay thế cơ chế quản lý dữ liệu cá nhân tại các hệ thống nguồn; các hệ thống nguồn vẫn giữ vai trò chủ trì dữ liệu theo quy định pháp luật.

Năm chức năng kỹ thuật chính:

- Cấp Hub ID vô danh cho công dân, tổ chức sau xác minh tại hệ thống nguồn;
- Phát hành, quản lý, thu hồi Chứng nhận xác minh (VC) theo chuẩn W3C Verifiable Credentials;
- Kiểm chứng VC cho các sản phẩm, cơ quan và bên kiểm chứng độc lập;
- Hỗ trợ truy vết theo yêu cầu pháp lý hợp lệ (đóng vai trò "chỉ đường", không "cung cấp thông tin");
- Ghi nhật ký bất biến mọi truy vấn Hub ID phục vụ giám sát việc tra cứu có đúng pháp luật hay không.

7.2. Kiến trúc cấu phần

Mô đun 7 gồm 05 hợp đồng thông minh và bộ cấu phần off-chain.

Bảng B.7.1. Hợp đồng thông minh của Mô đun 7

Hợp đồng	Chức năng
HubIDRegistry	Sổ đăng ký Hub ID; trạng thái xác minh, thời điểm cấp, khoá công khai tương ứng; không lưu thông tin cá nhân
VCRegistry	Sổ đăng ký các loại VC đang phát hành; schema từng loại; bên phát hành được ủy quyền
VCRevocationList	Danh sách VC đã bị thu hồi; cập nhật thời gian thực
IssuerWhitelist	Danh sách hệ thống nguồn được ủy quyền phát hành VC; phạm vi loại VC mỗi hệ thống
QueryLog	Nhật ký bất biến mọi truy vấn liên quan đến Hub ID

Các chuẩn tuân thủ: W3C DID Core (Decentralized Identifiers), W3C Verifiable Credentials Data Model **v2.0**, W3C Status List 2021, EIP-712.

Cấu phần off-chain gồm Hub ID Issuance Service (dịch vụ cấp Hub ID); VC Issuance and Verification Service; Wallet Gateway (kết nối với ví kỹ thuật số của người dùng); Reference Mapping Service (lưu ánh xạ Hub ID ↔ định danh tham chiếu tại hệ thống nguồn, đặt tại cơ sở của hệ thống nguồn, không tại Mô đun 7).

Cấu trúc dữ liệu Hub ID trên HubIDRegistry gồm sáu trường - tất cả không chứa thông tin cá nhân: hubId (chuỗi 32 byte sinh bằng keccak256); publicKey (khóa công khai do Mô đun 3 cấp); verificationLevel (mức xác minh tương ứng Mức 1 hoặc Mức 2 của VNeID theo Nghị định số 69/2024/NĐ-CP, hoặc tương đương đối với tổ chức); issuedAt; issuerRef (tham chiếu đến hệ thống nguồn - không phải danh tính); status (active / suspended / deactivated).

Mô đun 7 hỗ trợ đồng thời nhiều chuẩn định danh phi tập trung để không bị khoá vào một mô hình duy nhất: W3C DID Core v1.0, W3C VC Data Model **v2.0**, OpenID Connect for Verifiable Credential Issuance (OIDC4VCI), OpenID Connect for Verifiable Presentations (OIDC4VP); có thể hỗ trợ khung Self-Sovereign Identity theo EBSI của EU khi có nhu cầu liên thông quốc tế.

7.3. Quan hệ với các mô đun khác

Mô đun 7 là cơ sở hạ tầng định danh cho toàn bộ DNC-Chain. Mô đun 2 sử dụng Hub ID khi ghi bằng chứng liên quan đến người dùng. Mô đun 4 sử dụng Hub ID khi phát hành token cho người dùng. Mô đun 1 sử dụng Hub ID trong các thông điệp liên chuỗi liên quan đến người dùng, không truyền thông tin cá nhân qua cầu nối. Các sản phẩm SP2, SP4, SP5, SP7 sử dụng Hub ID và VC cho các tương tác với công dân. Quan hệ với Mô đun 3 mang tính nền tảng: Mô đun 3 cấp khoá mật mã cho Hub ID và quản lý phân quyền cho các hệ thống nguồn được phép phát hành VC.

7.4. Giao diện kỹ thuật chính

Bảng B.7.2. Giao diện chính của Mô đun 7

Nhóm giao diện	Chức năng	Chuẩn xác minh
Cấp Hub ID (Issuance API)	Hệ thống nguồn yêu cầu cấp Hub ID sau xác minh qua VNeID hoặc tương đương	mTLS + JWT + chữ ký số
Phát hành VC (VC Issuance API)	Hệ thống nguồn phát hành VC cho người dùng đã có Hub ID	mTLS + JWT + chữ ký số
Kiểm chứng VC (Verification API)	Bên kiểm chứng kiểm tra tính hợp lệ của VC	JWT hoặc không yêu cầu với VC công khai
Ví kỹ thuật số (Wallet API)	Người dùng quản lý Hub ID và VC của mình qua ví	Khóa riêng của người dùng
Truy vết pháp lý (Legal Lookup API)	Cơ quan có thẩm quyền yêu cầu tra cứu theo quy trình pháp luật	mTLS + JWT + xác nhận yêu cầu hợp lệ bằng chữ ký số cơ quan
Thu hồi VC (Revocation API)	Hệ thống nguồn thu hồi VC đã phát hành	mTLS + JWT + chữ ký số

Mô đun 7 áp dụng ba cơ chế tăng cường bảo vệ quyền riêng tư, áp dụng tùy trường hợp theo định hướng tại Phần A Mục X (Mở rộng và ứng dụng Zero-Knowledge):

- *Zero-Knowledge Proof (ZKP) tùy chọn*: cho phép công dân chứng minh thuộc tính (ví dụ "trên 18 tuổi", "có bằng đại học") mà không tiết lộ giá trị cụ thể;

- *Selective Disclosure*: khi xuất trình VC, công dân có thể chỉ tiết lộ một số trường cụ thể thay vì toàn bộ VC;

- *BBS+ Signatures*: chữ ký cho phép tổng hợp và xác minh các phần riêng lẻ của VC mà không cần tiết lộ toàn bộ, hỗ trợ Selective Disclosure.

7.5. Ràng buộc tuân thủ pháp lý

Mô đun 7 là mô đun có yêu cầu tuân thủ pháp lý cao nhất do liên quan trực tiếp đến dữ liệu cá nhân. Tuân thủ nghiêm ngặt:

- Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP (nguyên tắc thu thập tối thiểu; quyền chủ thể dữ liệu; quyền xóa dữ liệu thực hiện qua thu hồi VC);

- Luật Giao dịch điện tử số 20/2023/QH15 (tính pháp lý của chữ ký số phát hành VC);

- Luật An toàn thông tin mạng số 86/2015/QH13 (được sửa đổi, bổ sung bởi Luật số 35/2018/QH14) và Luật An ninh mạng số 24/2018/QH14, được hợp nhất và thay thế bởi Luật An ninh mạng số 116/2025/QH15 kể từ ngày 01/7/2026 (nhật ký bất biến; phân cấp bảo mật hệ thống);

- Các quy định của Bộ Công an về tích hợp với VNeID;

- Luật Tiếp cận thông tin (báo cáo công khai số lượng Hub ID, VC đã cấp, đã thu hồi, số truy vấn pháp lý - không chứa thông tin cá nhân).

Cơ chế quyền xóa dữ liệu thỏa hiệp hợp lý giữa tính bất biến của blockchain và quyền xóa dữ liệu cá nhân theo pháp luật: khi công dân yêu cầu xóa, hệ thống nguồn thẩm định, nếu chấp thuận thì (i) Mô đun 7 ghi VC vào VCRevocationList với lý do, (ii) hệ thống nguồn xóa mapping "định danh nội bộ ↔ Hub ID" tại cơ sở của hệ thống nguồn. Từ thời điểm này, Hub ID vẫn còn trên chuỗi nhưng không thể truy ngược về công dân do mapping đã bị xóa; VC bị vô hiệu hoá. Dữ liệu cá nhân thực sự (chỉ tồn tại tại hệ thống nguồn) được xóa.

7.6. Cơ chế nâng cấp

Các hợp đồng của Mô đun 7 áp dụng Proxy Upgrade Pattern qua Mô đun 5. Nâng cấp hợp đồng, thay đổi danh sách hệ thống nguồn trong IssuerWhitelist, thay đổi schema VC đều yêu cầu đa ký 3/5 và timelock 48 giờ. Toàn bộ thay đổi ghi vào QueryLog bất biến.

7.7. Chỉ tiêu mức dịch vụ cốt lõi

Bảng B.7.3. Chỉ tiêu mức dịch vụ của Mô đun 7

Chỉ tiêu	Mục tiêu
Thời gian sẵn sàng	$\geq 99,95\%$ hàng tháng (mô đun nền tảng về định danh)
Thời gian cấp Hub ID	≤ 5 giây
Thời gian phát hành VC	≤ 3 giây
Thời gian kiểm chứng VC	≤ 500 mili-giây
Thời gian xử lý yêu cầu truy vết pháp lý	≤ 60 giây
Thời gian thu hồi VC lan tỏa toàn mạng	≤ 30 giây

Chỉ tiêu	Mục tiêu
Tỷ lệ ghi nhật ký đầy đủ mọi truy vấn Legal Lookup API	100%

7.8. Điều kiện triển khai

- Kết nối kỹ thuật với VNeID đã được Bộ Công an chấp thuận và nghiệm thu;

Danh sách hệ thống nguồn được ủy quyền phát hành VC và phạm vi từng loại VC đã được ban hành bằng văn bản;

Schema cho từng loại VC đã được xác định theo chuẩn W3C VC Data Model **v2.0**;

Quy trình truy vết pháp lý đã được thống nhất với Công an thành phố và các cơ quan có thẩm quyền;

Kiểm toán độc lập tuân thủ nguyên tắc thu thập tối thiểu hoàn tất trước khi vận hành chính thức;

Giai đoạn 2026 - 2027 ưu tiên phục vụ các sản phẩm có dữ liệu cá nhân trong Tầng 1 (SP1, SP2); giai đoạn 2028 - 2030 hoàn thiện và mở rộng cho SP4 (hồ sơ y tế - yêu cầu bảo vệ dữ liệu cao), SP5 (sản dữ liệu), SP7 (loyalty) và các ứng dụng có yêu cầu xác minh, liên thông, bảo vệ dữ liệu khác.

TỔNG HỢP QUAN HỆ PHỤ THUỘC GIỮA 07 MÔ ĐUN VÀ 11 SẢN PHẨM

Bảng B.8.1 dưới đây tổng hợp quan hệ phụ thuộc giữa 07 mô đun nền tảng Phần B và **10 sản phẩm** ứng dụng Phần C, là bảng tra cứu quan trọng để xác định mức độ sử dụng từng mô đun cho từng sản phẩm.

Bốn cấp độ phụ thuộc được sử dụng trong bảng:

- **BB (Bắt buộc cốt lõi)**: Không có mô đun này thì sản phẩm không vận hành được.

- **B (Bắt buộc)**: Sản phẩm sử dụng mô đun ở mức chuẩn, không thể thay thế.

- **TC (Tùy chọn)**: Sản phẩm có thể sử dụng mô đun khi có nhu cầu cụ thể, được phê duyệt.

- **(Không sử dụng)**: Không sử dụng trong hạ tầng dùng chung; có thể sử dụng hạn chế theo cơ chế riêng đối với các sản phẩm Tầng 4.

Bảng B.8.1. Ma trận phụ thuộc 07 mô đun × 10 sản phẩm

Sản phẩm	M1 Cầu nối	M2 Bảng chứng	M3 Khóa & phân quyền	M4 Giao dịch & Token	M5 Smart contract	M6 Ứng dụng & marketplace	M7 Hub dữ liệu

Sản phẩm	M1 Câu nối	M2 Bằng chứng	M3 Khóa & phân quyền	M4 Giao dịch & Token	M5 Smart contract	M6 Ứng dụng & marketplace	M7 Hub dữ liệu
SP1 - Toàn vẹn hồ sơ điện tử	TC	BB	B	-	B	B	B
SP2 - Xác minh văn bằng, chứng chỉ	TC	BB	B	B	B	B	BB
SP3 - Bản sao số đô thị (Digital Twin)	TC	B	B	TC	B	B	TC
SP8 - Xác minh hồ sơ y tế	TC	BB	B	TC	B	B	BB
SP3 - Sàn giao dịch dữ liệu thành phố	TC	B	B	B	B	B	B
SP4 - Sàn giao dịch tài sản sở hữu trí tuệ	B	B	B	BB	B	B	B
SP5 - Khách hàng trung thành thành phố	TC	TC	B	BB	B	B	B

Sản phẩm	M1 Cầu nối	M2 Bảng chứng	M3 Khóa & phân quyền	M4 Giao dịch & Token	M5 Smart contract	M6 Ứng dụng & marketplace	M7 Hub dữ liệu
SP6 - Chuyển đổi TSMH sang tiền pháp định	-	-	TC	TC (cơ chế riêng, chỉ ConversionGateway)	TC	TC	TC
SP7 - Phát hành, lưu ký và giao dịch TSMH (RWA)	-	-	TC	TC (cơ chế riêng)	TC	TC	TC
SP9 - Gọi vốn cộng đồng	-	-	TC	TC (cơ chế riêng)	TC	TC	TC

Ghi chú áp dụng đối với Bảng B.8.1:

SP8, SP9, SP10 thuộc Tầng 4 của Đề án, triển khai theo cơ chế riêng gắn với Trung tâm tài chính quốc tế tại Việt Nam hoặc cơ chế sandbox theo Nghị quyết số 55/2024/NQ-HĐND ngày 13/12/2024 của Hội đồng nhân dân thành phố. Các mức "TC" tại ba sản phẩm này chỉ áp dụng trong phạm vi cho phép của cơ chế riêng; ba sản phẩm này không có hợp đồng thông minh triển khai mới trên hạ tầng dùng chung, chỉ sử dụng các cầu phần giao tiếp đã được phê duyệt của Mô đun 4 (ConversionGateway) và các mô đun khác trong phạm vi hỗ trợ kỹ thuật.

SP6 là sản phẩm duy nhất có Mô đun 1 (Cầu nối đa chuỗi) ở mức bắt buộc do đặc thù nhu cầu liên thông bằng chứng sở hữu trí tuệ với chuỗi ngoài khi có nhu cầu quốc tế hoá, và là sản phẩm duy nhất có Mô đun 4 ở mức bắt buộc cốt lõi do bản chất sản phẩm là quản lý token đại diện quyền sở hữu trí tuệ có thể chuyển nhượng có kiểm soát.

Mô đun 3 (Quản lý khoá và phân quyền), Mô đun 5 (Quản lý smart contract) và Mô đun 6 (Quản lý ứng dụng) được 07 trong 10 sản phẩm sử dụng ở mức bắt buộc hoặc cao hơn (trừ các sản phẩm Tầng 4 sử dụng theo cơ chế riêng), phản ánh vai trò nền tảng xuyên suốt của ba mô đun này đối với toàn bộ hạ tầng.

Chi tiết kỹ thuật về cách từng sản phẩm tích hợp với các mô đun tương ứng được trình bày tại Phần C.

PHẦN C: THUYẾT MINH KỸ THUẬT 10 SẢN PHẨM ỨNG DỤNG

Phần C thuyết minh kỹ thuật 10 sản phẩm ứng dụng được triển khai trên hạ tầng DNC-Chain theo 04 tầng cấp độ đã xác định tại Bảng 3 Mục IV Chương III của Đề án. Nội dung Phần C tập trung vào kiến trúc kỹ thuật, hợp đồng thông minh riêng, giao diện tích hợp, chỉ tiêu kỹ thuật và điều kiện triển khai đặc thù của từng sản phẩm; không lặp lại nội dung nghiệp vụ đã mô tả tại Chương IV Mục III của Đề án và không lặp lại đặc tả kỹ thuật của 07 mô đun nền tảng đã trình bày tại Phần B.

Năm nguyên tắc sau bổ sung cho 05 nguyên tắc cơ bản của DNC-Chain tại Khoản 2 Mục I Phần A, áp dụng riêng cho sản phẩm ứng dụng trên DNC-Chain; áp dụng thống nhất cho cả 10 sản phẩm, không lặp lại tại từng mục sản phẩm:

1. Kiến trúc hai lớp thống nhất. Mỗi sản phẩm tổ chức theo kiến trúc hai lớp. Lớp off-chain đặt tại hạ tầng dữ liệu của thành phố hoặc của cơ quan, đơn vị chủ trì sản phẩm, chịu trách nhiệm xử lý nghiệp vụ, chuẩn hóa dữ liệu, tính giá trị băm và giao tiếp với người dùng cuối. Lớp on-chain gồm các hợp đồng thông minh riêng của sản phẩm triển khai trên DNC-Chain, chịu trách nhiệm ghi nhận bằng chứng mật mã, lưu vết bất biến và kiểm chứng. Hai lớp kết nối với các mô đun nền tảng dùng chung thông qua các giao diện đã đặc tả tại Phần B.

2. Tích hợp ngang hàng với LGSP. Mỗi sản phẩm là ứng dụng nghiệp vụ độc lập, tích hợp ngang hàng với nền tảng tích hợp và chia sẻ dữ liệu của thành phố (LGSP) theo Nghị định số 278/2025/NĐ-CP của Chính phủ về quản trị dữ liệu, kết nối, chia sẻ, sử dụng dữ liệu của cơ quan nhà nước và Khung kiến trúc dữ liệu quốc gia tại Quyết định số 2439/QĐ-TTg. Sản phẩm trên DNC-Chain không thay thế hệ thống nguồn, không thay thế cơ sở dữ liệu chuyên ngành và không thay thế quy trình nghiệp vụ hiện có.

3. Bảo vệ dữ liệu cá nhân và nguyên tắc thu thập tối thiểu. Chỉ các trường siêu dữ liệu kỹ thuật, giá trị băm (hash), mã định danh vô danh (Hub ID), mã tham chiếu giao dịch và trạng thái xác minh được ghi lên DNC-Chain. Các trường dữ liệu cá nhân (họ tên, số định danh cá nhân, ngày sinh, địa chỉ, dữ liệu sinh trắc học), dữ liệu cá nhân nhạy cảm theo Điều 3 Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, nội dung chi tiết hồ sơ, kết quả xét nghiệm, chẩn đoán y tế, đơn thuốc, bảng điểm chi tiết, nội dung hợp đồng, số dư tài khoản và tương đương không được ghi lên chuỗi trong mọi trường hợp. Danh sách trường cá nhân loại trừ chi tiết của từng sản phẩm được cơ quan chủ trì dữ liệu nguồn ban hành bằng quyết định trước khi đưa vào vận hành.

4. Sử dụng mô đun dùng chung, không tái tạo chức năng. Không sản phẩm nào được tái tạo chức năng đã có tại Phần B. Các thao tác dùng chung (ghi bằng chứng, phát hành token, quản lý khoá, phân quyền, nâng cấp hợp đồng, cấp Hub ID, phát hành chứng thư số) đều ủy thác cho mô đun tương ứng. Phần đặc thù của sản phẩm chỉ gồm các hợp đồng thông minh riêng và các cấu phần off-chain riêng, không trùng lặp với các mô đun nền tảng. Mức độ phụ thuộc từng mô đun được ghi rõ tại Mục "Phụ thuộc mô đun" của từng sản phẩm, căn cứ Bảng B.8.1.

5. Kiểm toán bảo mật tuân thủ quy định chung. Toàn bộ hợp đồng thông minh riêng, cấu phần off-chain và giao diện tích hợp của từng sản phẩm phải được kiểm toán bảo mật độc lập theo quy định chung tại Phần A Mục XII trước khi đưa vào vận hành

chính thức; kiểm toán lặp lại sau mỗi lần nâng cấp lớn. Nội dung chi tiết về quy trình, tần suất, phạm vi và đơn vị kiểm toán không lặp lại tại từng mục sản phẩm.

Phần C được trình bày theo thứ tự 04 tầng: Tầng 1 gồm SP1, SP2 (triển khai 2026 - 2027); Tầng 2 gồm SP3, SP8 (triển khai 2028 - 2030); Tầng 3 gồm SP3, SP4, SP5 (triển khai 2028 - 2030); Tầng 4 gồm SP6, SP7, SP9 (triển khai theo cơ chế riêng gắn với Trung tâm tài chính quốc tế tại Việt Nam hoặc cơ chế sandbox). Mỗi sản phẩm được thuyết minh theo khuôn mẫu thống nhất gồm 07 mục: định vị sản phẩm; chức năng nghiệp vụ chính; kiến trúc kỹ thuật đặc thù; phụ thuộc mô đun; giao diện và tích hợp; chỉ tiêu kỹ thuật cốt lõi; điều kiện triển khai và giới hạn phạm vi.

SP1 - Hệ thống bảo đảm toàn vẹn hồ sơ điện tử trên blockchain

1. Định vị sản phẩm

SP1 thuộc Tầng 1 của Đề án, triển khai trong giai đoạn 2026 - 2027. Sản phẩm ghi nhận bằng chứng toàn vẹn của hồ sơ điện tử và chuỗi sự kiện xử lý hồ sơ trong quá trình tiếp nhận, luân chuyển, xử lý, chia sẻ giữa các cơ quan, đơn vị, phục vụ đối soát, kiểm chứng, tra cứu và hậu kiểm. SP1 là ứng dụng nghiệp vụ độc lập, tích hợp ngang hàng với LGSP, không thay thế hệ thống nguồn và không lưu trữ hồ sơ điện tử gốc.

Vai trò của DNC-Chain trong SP1 là lớp tin cậy số ghi nhận bằng chứng mật mã (hash) và siêu dữ liệu tham chiếu. Hồ sơ điện tử gốc tiếp tục được quản lý tại hệ thống nguồn theo Luật Giao dịch điện tử số 20/2023/QH15 và Luật Dữ liệu số 60/2024/QH15.

2. Chức năng nghiệp vụ chính

SP1 cung cấp sáu nhóm chức năng:

- Ghi bằng chứng toàn vẹn hồ sơ điện tử tại thời điểm tạo lập và mọi điểm thay đổi trạng thái;
- Ghi chuỗi sự kiện xử lý hồ sơ theo trình tự thời gian (tạo lập, chuyển tiếp, xử lý, trả kết quả, lưu trữ, hủy);
- Kiểm chứng tính toàn vẹn hồ sơ theo yêu cầu qua cổng tra cứu công khai hoặc API;
- Đối soát trạng thái hồ sơ liên sở, liên ngành phục vụ giám sát, thanh tra, kiểm toán;
- Phát hiện và cảnh báo điểm nghẽn xử lý khi thời gian xử lý vượt ngưỡng quy định;
- Chia sẻ bằng chứng với chuỗi ngoài phục vụ đối soát liên tỉnh qua VBSN khi có nhu cầu và được cấp có thẩm quyền phê duyệt.

3. Kiến trúc kỹ thuật đặc thù

SP1 tổ chức theo kiến trúc hai lớp: lớp off-chain đặt tại hạ tầng dữ liệu của cơ quan chủ trì sản phẩm và lớp on-chain gồm hai hợp đồng thông minh riêng trên DNC-Chain.

Bảng C.1.1. Cấu phần off-chain và on-chain của SP1

Lớp	Cấu phần	Chức năng kỹ thuật chính
-----	----------	--------------------------

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Integration Gateway	Tiếp nhận dữ liệu hồ sơ qua LGSP; chuẩn hoá; loại bỏ trường cá nhân theo danh sách trường loại trừ trước khi băm
Off-chain	Hash Computation Service	Tính SHA-256 của nội dung hồ sơ, keccak256 của mã định danh bằng chứng; gắn dấu thời gian theo RFC 3161
Off-chain	Event Reconciliation Engine	Theo dõi chuỗi sự kiện xử lý hồ sơ; phát hiện điểm nghẽn; cảnh báo khi vượt ngưỡng mức dịch vụ
Off-chain	Verification Portal và Reconciliation Dashboard	Cổng tra cứu công khai (không yêu cầu tài khoản với bằng chứng công khai); giao diện đối soát cho cơ quan giám sát
Off-chain	Integration SDK	Thư viện tích hợp Java, Node.js, Python, .NET cho hệ thống nguồn
On-chain	DocProofRegistry	Hợp đồng thông minh riêng; lưu bằng chứng toàn vẹn hồ sơ (hash, siêu dữ liệu, chữ ký); kế thừa ProofRegistryTemplate của Mô đun 5
On-chain	DocEventLog	Hợp đồng thông minh riêng; ghi chuỗi sự kiện xử lý hồ sơ theo trình tự thời gian với tham chiếu sự kiện liền trước

Hai hợp đồng thông minh riêng tuân thủ EIP-712 (ký dữ liệu có cấu trúc), ERC-165 (phát hiện interface) và EIP-1967 (Proxy Storage). Cấu trúc dữ liệu bằng chứng trên DocProofRegistry gồm các trường kỹ thuật (proofId, docHash, docTypeCode, docRefId, timestamp, metadataURI, chữ ký số); danh sách trường dữ liệu cá nhân loại trừ (họ tên, số định danh cá nhân, ngày sinh, địa chỉ, nội dung toàn văn văn hồ sơ, hình ảnh, ghi chú nội bộ, dữ liệu cá nhân nhạy cảm theo Điều 3 Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15) không được ghi lên chuỗi trong mọi trường hợp; danh sách chi tiết theo nhóm hồ sơ do cơ quan chủ trì dữ liệu nguồn ban hành bằng quyết định trước khi đưa vào vận hành.

Luồng kỹ thuật cơ bản: khi hồ sơ điện tử được tạo lập hoặc thay đổi trạng thái tại hệ thống nguồn, dữ liệu cần xác minh được chuyển qua LGSP đến Integration Gateway. Integration Gateway loại bỏ các trường cá nhân, tính hash qua Hash Computation Service, ghi bằng chứng lên DocProofRegistry theo cơ chế gom lô của BatchManager - Mô đun 2 (ghi Merkle Root của lô thay vì từng bằng chứng riêng lẻ, tối ưu chi phí giao dịch). Sự kiện xử lý hồ sơ tiếp theo (chuyển tiếp, trả kết quả, lưu trữ) được ghi lên

DocEventLog với tham chiếu đến sự kiện liền trước, hình thành chuỗi sự kiện có thể truy vết. Khi có yêu cầu kiểm chứng, Verification Portal tra bằng chứng gốc, tính lại hash từ dữ liệu hiện có và so sánh; kết quả kiểm chứng được ghi vào VerificationLog của Mô đun 2.

SP1.4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP1: M1: TC; M2: BB; M3: B; M4: -; M5: B; M6: B; M7: B.

- **Mô đun 2 (bắt buộc cốt lõi):** DocProofRegistry gọi ProofRegistry và BatchManager để ghi bằng chứng theo cơ chế gom lô. Đây là mô đun quyết định khả năng xử lý khối lượng hồ sơ lớn với chi phí tối ưu; không thay thế được.

- **Mô đun 3 (bắt buộc):** phân quyền ROLE_ISSUER cho hệ thống nguồn được phép ghi bằng chứng, ROLE_VERIFIER cho cán bộ kiểm chứng, ROLE_AUDITOR cho cơ quan giám sát.

- **Mô đun 5 (bắt buộc):** hai hợp đồng thông minh riêng đăng ký vào ContractRegistry; nâng cấp theo Proxy Upgrade Pattern với đa ký và timelock tối thiểu 48 giờ.

- **Mô đun 6 (bắt buộc):** SP1 đăng ký vào ApplicationRegistry; trạng thái vòng đời quản lý bởi LifecycleManager; công bố trên Marketplace Portal.

- **Mô đun 7 (bắt buộc):** với hồ sơ liên quan đến công dân, trường subjectHubId trên DocProofRegistry là Hub ID vô danh do Mô đun 7 cấp, không phải thông tin cá nhân.

Mức tùy chọn Mô đun 1 áp dụng khi cần chia sẻ bằng chứng liên tỉnh qua VBSN: DocProofRegistry chuyển Merkle Proof qua Mô đun 1 theo danh sách chuỗi được phép; không chuyển hồ sơ gốc, không chuyển thông tin cá nhân.

5. Giao diện và tích hợp

SP1 tích hợp với hệ thống nguồn qua LGSP theo Nghị định số 278/2025/NĐ-CP. Ba nhóm hệ thống nguồn trong giai đoạn đầu: hệ thống dịch vụ công trực tuyến của thành phố (các nhóm thủ tục hành chính tần suất cao); hệ thống nghiệp vụ chuyên ngành của các sở - ban - ngành (hồ sơ thuộc thẩm quyền xử lý của cơ quan); hệ thống quản lý văn bản và điều hành (văn bản điện tử có chữ ký số, quyết định hành chính).

Bảng C.1.2. Giao diện kỹ thuật chính của SP1

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Hệ thống nguồn qua LGSP	REST trên HTTPS; webhook nhận biên lai xác minh	mTLS + JWT + chữ ký số ERC-191 của hệ thống nguồn
Hệ thống nguồn tích hợp trực tiếp	Integration SDK (Java, Node.js, Python, .NET)	OAuth 2.0 Client Credentials Grant qua Mô đun 3

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Cán bộ kiểm chứng, cơ quan giám sát	Reconciliation Dashboard	JWT + ROLE_VERIFIER hoặc ROLE_AUDITOR
Bên kiểm chứng độc lập	Verification Portal công khai; API kiểm chứng mở	Không bắt buộc với bằng chứng công khai; API key + rate limit với API mở
Chuỗi ngoài khi đối soát liên tỉnh (VBSN)	Qua Mô đun 1 - Cầu nối đa chuỗi	Theo đặc tả Mô đun 1 tại Phần B Mục 1

Chuẩn kỹ thuật cốt lõi áp dụng thống nhất: JSON-LD theo W3C Verifiable Credentials Data Model **v2.0** cho định dạng dữ liệu; Dublin Core cho siêu dữ liệu; RFC 3161 cho dấu thời gian; ECDSA trên đường cong secp256k1 cho chữ ký số; SHA-256 cho nội dung hồ sơ và keccak256 cho định danh bằng chứng; Khung kiến trúc dữ liệu quốc gia theo Quyết định số 2439/QĐ-TTg. Các chuẩn này áp dụng thống nhất theo quy định chung tại Phần A Mục VII và Mục XII.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.1.3. Chỉ tiêu mức dịch vụ cốt lõi của SPI

Chỉ tiêu	Mức cam kết
Thời gian ghi bằng chứng (từ khi nhận dữ liệu qua LGSP đến khi trả biên lai)	≤ 30 giây với 99% bằng chứng tính theo tháng
Thời gian kiểm chứng toàn vẹn qua Verification Portal	≤ 3 giây với 99,5% lượt tính theo tháng
Tỷ lệ ghi bằng chứng thành công (không tính lỗi phía hệ thống nguồn)	≥ 99,9% tính theo tháng
Khả năng chịu tải (chế độ gom lô)	≥ 500 bằng chứng/giây
Thời gian sẵn sàng của Integration Gateway	≥ 99,9% tính theo tháng
Thời gian sẵn sàng của Verification Portal	≥ 99,5% tính theo tháng

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút) áp dụng theo quy định chung tại Phần A Mục VII.

7. Điều kiện triển khai và giới hạn phạm vi

Điều kiện kỹ thuật triển khai SP1:

- Hệ thống nguồn tích hợp đã có khả năng ký số ECDSA secp256k1 và đã đăng ký chứng thư số vào KeyRegistry của Mô đun 3;
- Dữ liệu hồ sơ tại hệ thống nguồn đã được chuẩn hoá theo Khung kiến trúc dữ liệu quốc gia;
- Mã hồ sơ và loại hồ sơ đã được đăng ký vào IssuerRegistry của Mô đun 2 với phạm vi loại bằng chứng được phép tạo đã được phê duyệt bằng văn bản;
- LGSP đã cấp kênh kết nối mTLS đến Integration Gateway của SP1;
- Cơ quan chủ trì dữ liệu nguồn đã ban hành quyết định danh sách trường cá nhân loại trừ trước khi đưa vào vận hành;
- Hai hợp đồng DocProofRegistry và DocEventLog đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;

SP1 đã được đăng ký vào ApplicationRegistry của Mô đun 6 và chuyển sang trạng thái vận hành chính thức theo LifecycleManager.

Giới hạn phạm vi đặc tả của Phụ lục đối với SP1. Các nội dung sau thuộc hồ sơ thiết kế kỹ thuật dự án thành phần hoặc tài liệu vận hành, không thuộc phạm vi Phụ lục I:

- Danh sách cụ thể các nhóm hồ sơ điện tử đưa vào triển khai trong giai đoạn đầu và lộ trình mở rộng theo từng năm;
- Danh sách trường cá nhân loại trừ chi tiết cho từng nhóm hồ sơ;
- Tham số cấu hình chi tiết của các cấu phần off-chain (kích thước lô, chu kỳ gom, số lần thử lại, độ trễ đồng bộ, ngưỡng cảnh báo theo từng nhóm hồ sơ);
- Thiết kế chi tiết giao diện người dùng của Verification Portal và Reconciliation Dashboard;
- Quy trình phối hợp nghiệp vụ cụ thể giữa cơ quan chủ trì sản phẩm, cơ quan chủ trì dữ liệu nguồn và các cơ quan giám sát;
- Kế hoạch ứng cứu sự cố và diễn tập cụ thể của SP1 (áp dụng khung chung tại Phần A Mục VII).

SP2 - Hệ thống xác minh văn bằng, chứng chỉ trên blockchain

1. Định vị sản phẩm

SP2 thuộc Tầng 1 của Đề án, triển khai trong giai đoạn 2026 - 2027. Sản phẩm là nền tảng xác minh văn bằng, chứng chỉ dùng chung cho các cơ sở giáo dục trên địa bàn thành phố, thực hiện hai chức năng kỹ thuật cốt lõi: ghi nhận bằng chứng xác minh đối với văn bằng đã được cơ sở đào tạo phát hành hợp lệ; và phát hành Chứng nhận xác minh

(Verifiable Credential - VC) gắn với Token định danh văn bằng không thể chuyển nhượng (Soulbound Token - SBT) cho người học.

Vai trò của DNC-Chain trong SP2 là lớp tin cậy số ghi nhận bằng chứng và lưu trữ bất biến trạng thái hiệu lực của văn bằng. Blockchain không thay đổi thẩm quyền cấp bằng, không làm phát sinh nghĩa vụ pháp lý mới đối với cơ sở đào tạo; văn bằng gốc tiếp tục do cơ sở đào tạo cấp và quản lý theo thẩm quyền quy định tại Luật Giáo dục, Luật Giáo dục đại học, Luật Giáo dục nghề nghiệp và Thông tư số 10/2026/TT-BGDĐT của Bộ Giáo dục và Đào tạo về mã văn bằng, mã chứng chỉ.

2. Chức năng nghiệp vụ chính

SP2 cung cấp sáu nhóm chức năng:

- Ghi bằng chứng xác minh của văn bằng, chứng chỉ khi cơ sở đào tạo phát hành hợp lệ;
- Đúc Token định danh văn bằng (SBT) gắn với Hub ID vô danh của người học;
- Phát hành Chứng nhận xác minh về văn bằng cho người học theo chuẩn W3C Verifiable Credentials;
- Xác minh văn bằng qua cổng xác minh công khai (nhập số hiệu hoặc quét mã QR);
- Xác minh qua Chứng nhận xác minh do người học xuất trình, hỗ trợ tiết lộ có chọn lọc (Selective Disclosure);

Thu hồi hoặc đình chỉ hiệu lực văn bằng theo quyết định của cơ sở đào tạo.

3. Kiến trúc kỹ thuật đặc thù

SP2 tổ chức theo kiến trúc hai lớp: lớp off-chain đặt tại hạ tầng dữ liệu của cơ sở đào tạo hoặc của cơ quan chủ trì sản phẩm và lớp on-chain gồm **ba hợp đồng thông minh riêng** trên DNC-Chain.

Bảng C.2.1. Cấu phần off-chain và on-chain của SP2

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Credential Integration Gateway	Tiếp nhận dữ liệu văn bằng chuẩn hoá từ phần mềm quản lý đào tạo qua LGSP; loại bỏ trường cá nhân chi tiết theo danh sách trường loại trừ
Off-chain	Credential Hash Engine	Tính SHA-256 của khối dữ liệu văn bằng chuẩn hoá; sinh proofId theo keccak256; gắn dấu thời gian RFC 3161
Off-chain	VC Issuance Service	Phát hành Chứng nhận xác minh theo W3C VC Data Model v2.0; ký số bằng khóa riêng của cơ sở đào tạo

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Holder Wallet	Ví định danh số của người học; lưu và xuất trình VC khi cần xác minh; hỗ trợ tiết lộ có chọn lọc
Off-chain	Verification Portal	Cổng xác minh công khai (nhập số hiệu văn bằng hoặc quét mã QR)
Off-chain	Employer Integration API	Giao diện tích hợp với phần mềm quản trị nhân sự và tuyển dụng của doanh nghiệp
On-chain	DegreeRegistry	Hợp đồng thông minh riêng; đúc và quản lý SBT văn bằng gắn với Hub ID người học; kế thừa TokenStandardTemplate của Mô đun 5
On-chain	DegreeProofRegistry	Hợp đồng thông minh riêng; ghi bằng chứng băm của dữ liệu văn bằng; kế thừa ProofRegistryTemplate của Mô đun 5
On-chain	DegreeRevocationList	Hợp đồng thông minh riêng; danh sách văn bằng bị thu hồi hoặc đình chỉ; đánh dấu trạng thái, không xóa bản ghi gốc

Ba hợp đồng thông minh riêng tuân thủ các chuẩn: ERC-721 với thuộc tính transferable=false (SBT), EIP-712 (ký dữ liệu có cấu trúc), ERC-165 (phát hiện interface), EIP-1967 (Proxy Storage), W3C Status List 2021 (quản lý trạng thái thu hồi), RFC 5280 (CRL compatible). Cấu trúc dữ liệu SBT trên DegreeRegistry gồm các trường kỹ thuật (tokenId, holderHubId, issuerDID, degreeTypeCode theo Thông tư số 10/2026/TT-BGDĐT, degreeRefHash, issueDate, metadataURI, statusCode, thuộc tính transferable luôn nhận giá trị false). Danh sách trường dữ liệu cá nhân loại trừ không được ghi lên chuỗi gồm: họ tên đầy đủ, số định danh cá nhân, ngày sinh, nơi sinh, dân tộc, quốc tịch của người học; bảng điểm chi tiết, điểm từng học phần, điểm trung bình tích lũy, xếp loại chi tiết môn; hình ảnh văn bằng, hình ảnh chữ ký, hình ảnh bản sao; hồ sơ dự tuyển, lý lịch sinh viên, thông tin gia đình; dữ liệu cá nhân nhạy cảm theo Điều 3 Luật số 91/2025/QH15.

Luồng kỹ thuật cơ bản: khi cơ sở đào tạo phát hành văn bằng theo quy trình của cơ sở, dữ liệu văn bằng chuẩn hoá theo Thông tư số 10/2026/TT-BGDĐT được chuyển qua LGSP đến Credential Integration Gateway. Gateway xác minh cơ sở đào tạo qua IssuerWhitelist của Mô đun 7 và IssuerRegistry của Mô đun 2, loại trừ trường cá nhân, tính hash qua Credential Hash Engine. Bằng chứng băm được ghi lên DegreeProofRegistry theo cơ chế gom lô của BatchManager - Mô đun 2. Đồng thời, DegreeRegistry gọi TokenFactory - Mô đun 4 đúc SBT với holderHubId là Hub ID của người học; ComplianceEngine - Mô đun 4 kiểm tra trạng thái ROLE_DEGREE_ISSUER

trước mỗi lần đúc token và chặn mọi lời gọi chuyển nhượng. VC Issuance Service phát hành Chứng nhận xác minh ký bằng khóa riêng của cơ sở đào tạo, đăng ký vào VRegistry của Mô đun 7; người học tiếp nhận VC vào ví định danh số. Khi có yêu cầu xác minh, bên xác minh có thể tra cứu công khai qua Verification Portal (dùng số hiệu văn bằng hoặc quét mã QR), hoặc yêu cầu người học xuất trình Chứng nhận xác minh qua luồng OIDC4VP của Mô đun 7. Khi thu hồi, cơ sở đào tạo có ROLE_DEGREE_REVOKER ghi trạng thái lên DegreeRevocationList; DegreeRegistry cập nhật statusCode của SBT tương ứng (không đốt token để lưu lịch sử đầy đủ); Mô đun 7 cập nhật VRevocationList theo W3C Status List 2021.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP2: M1: TC; M2: BB; M3: B; M4: B; **M5: B; M6: B; M7: BB.**

Mô đun 2 (bắt buộc cốt lõi): DegreeProofRegistry gọi ProofRegistry và BatchManager Mô đun 2 để ghi bằng chứng theo cơ chế gom lô, tối ưu chi phí giao dịch lúc cao điểm đợt tốt nghiệp.

Mô đun 7 (bắt buộc cốt lõi): người học được định danh bằng Hub ID của Mô đun 7, không dùng họ tên, số định danh cá nhân trên chuỗi; Chứng nhận xác minh về văn bằng đăng ký vào VRegistry; các cơ sở đào tạo tham gia hệ thống đăng ký vào IssuerWhitelist. Mô đun 7 cũng là điểm kết nối của luồng xác minh OIDC4VP.

Mô đun 3 (bắt buộc): quản lý các vai trò ROLE_DEGREE_ISSUER (cơ sở đào tạo được ủy quyền phát hành), ROLE_DEGREE_REVOKER (cơ sở được thu hồi), ROLE_EMPLOYER_VERIFIER (tổ chức tuyển dụng được tích hợp), ROLE_DEGREE_AUDITOR (cơ quan quản lý giám sát).

Mô đun 4 (bắt buộc): DegreeRegistry sử dụng TokenFactory Mô đun 4 đúc Token định danh văn bằng theo chuẩn ERC-721 với transferable=false (SBT). ComplianceEngine chặn tuyệt đối mọi lời gọi chuyển nhượng - đây là ràng buộc kỹ thuật không thể vượt qua, bảo đảm văn bằng không trở thành tài sản có thể mua bán.

Mô đun 5 (bắt buộc): ba hợp đồng thông minh riêng đăng ký vào ContractRegistry; nâng cấp theo Proxy Upgrade Pattern với đa ký và timelock tối thiểu 48 giờ.

Mô đun 6 (bắt buộc): SP2 đăng ký vào ApplicationRegistry; trạng thái vòng đời quản lý bởi LifecycleManager; công bố trên Marketplace Portal.

Mức tùy chọn Mô đun 1 áp dụng khi mở rộng liên thông xác minh văn bằng ra ngoài phạm vi thành phố: Merkle Proof được chia sẻ qua Mô đun 1 theo danh sách chuỗi được phép, không chuyển dữ liệu văn bằng gốc, không chuyển thông tin cá nhân người học.

5. Giao diện và tích hợp

SP2 tích hợp với phần mềm quản lý đào tạo của các cơ sở giáo dục đại học, cao đẳng, trung cấp, cơ sở giáo dục nghề nghiệp trên địa bàn thành phố qua LGSP theo Nghị định số 278/2025/NĐ-CP. Ba nhóm hệ thống nguồn: phần mềm quản lý đào tạo của cơ sở giáo dục đại học (văn bằng cử nhân, kỹ sư, thạc sĩ, tiến sĩ); phần mềm quản lý đào tạo của

cơ sở giáo dục nghề nghiệp (văn bằng cao đẳng, trung cấp, chứng chỉ nghề); hệ thống cấp chứng chỉ chuyên môn của các cơ sở được giao cấp chứng chỉ theo quy định chuyên ngành.

Bảng C.2.2. Giao diện kỹ thuật chính của SP2

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Phần mềm quản lý đào tạo qua LGSP	REST trên HTTPS; webhook nhận biên lai phát hành SBT và VC	mTLS + JWT + chữ ký số ERC-191 của cơ sở đào tạo
Người học	Holder Wallet; luồng xuất trình VC theo OIDC4VP	Khóa riêng của người học
Nhà tuyển dụng, doanh nghiệp	Employer Integration API; Verification API của Mô đun 7	JWT + ROLE_EMPLOYER_VERIFIER (với cơ chế tích hợp); API key với xác minh công khai
Bên xác minh độc lập	Verification Portal công khai (nhập số hiệu văn bằng hoặc quét mã QR)	Không bắt buộc với xác minh công khai
Cơ quan quản lý, giám sát	Giao diện quản trị và báo cáo	JWT + ROLE_DEGREE_AUDITOR

Chuẩn kỹ thuật cốt lõi: W3C DID Core v1.0 cho mô hình định danh người học; W3C Verifiable Credentials Data Model v2.0 cho Chứng nhận xác minh; lược đồ siêu dữ liệu văn bằng tham chiếu European Learning Model hoặc lược đồ do Bộ Giáo dục và Đào tạo ban hành; OpenID Connect for Verifiable Credential Issuance (OIDC4VCI) và OpenID Connect for Verifiable Presentations (OIDC4VP) cho luồng phát hành và xác minh; ERC-721 với transferable=false cho SBT; W3C Status List 2021 cho trạng thái thu hồi; Thông tư số 10/2026/TT-BGDĐT cho mã văn bằng, mã chứng chỉ. Các chuẩn mật mã chung (ECDSA secp256k1, SHA-256, keccak256, RFC 3161) áp dụng thống nhất theo quy định tại Phần A Mục VII.

SP2.6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.2.3. Chỉ tiêu mức dịch vụ cốt lõi của SP2

Chỉ tiêu	Mức cam kết
-----------------	--------------------

Chỉ tiêu	Mức cam kết
Thời gian đúc SBT và ghi bằng chứng từ khi nhận dữ liệu qua LGSP	≤ 60 giây với 99% văn bằng tính theo tháng
Thời gian xác minh qua Verification Portal	≤ 3 giây với 99,5% lượt tính theo tháng
Thời gian xác minh qua luồng OIDC4VP (VC do người học xuất trình)	≤ 5 giây với 99% lượt tính theo tháng
Tỷ lệ ghi bằng chứng thành công	$\geq 99,9\%$ tính theo tháng
Khả năng chịu tải lúc cao điểm đợt tốt nghiệp	≥ 100 văn bằng/giây ở chế độ gom lô
Số lượt xác minh đáp ứng	≥ 25.000 lượt/năm giai đoạn đầu; ≥ 50.000 lượt/năm giai đoạn mở rộng

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút) áp dụng theo quy định chung tại Phần A Mục VII. Thời gian xác minh văn bằng tính theo chỉ tiêu mức dịch vụ của SP2 (≤ 5 giây qua OIDC4VP, ≤ 3 giây qua Portal) bảo đảm mục tiêu thời gian xác minh không quá 01 ngày đã dự kiến tại Chương III Mục III của Đề án.

7. Điều kiện triển khai và giới hạn phạm vi

Điều kiện kỹ thuật triển khai SP2:

- Dữ liệu văn bằng, chứng chỉ tại cơ sở đào tạo đã được chuẩn hoá theo Thông tư số 10/2026/TT-BGDĐT;
- Cơ sở đào tạo đã được đăng ký vào IssuerWhitelist của Mô đun 7 và IssuerRegistry của Mô đun 2 với phạm vi loại văn bằng được phép cấp, có quyết định phê duyệt bằng văn bản;
- Khóa ký số của cơ sở đào tạo đã được đăng ký vào KeyRegistry của Mô đun 3; HSM của cơ sở đào tạo đạt quy chuẩn tương đương FIPS 140-3 Level 3 theo yêu cầu tại Phần A Mục VII, ưu tiên thiết bị trong nước đã được Ban Cơ yếu Chính phủ chứng nhận;
- LGSP đã cấp kênh kết nối mTLS đến Credential Integration Gateway;
- Cơ quan chủ trì sản phẩm đã ban hành lược đồ tiêu dữ liệu văn bằng và danh sách trường cá nhân loại trừ;
- Ba hợp đồng DegreeRegistry, DegreeProofRegistry, DegreeRevocationList đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;

- SP2 đã được đăng ký vào ApplicationRegistry của Mô đun 6 và chuyển sang trạng thái vận hành chính thức theo LifecycleManager.

Giới hạn phạm vi đặc tả của Phụ lục đối với SP2. Các nội dung sau thuộc hồ sơ thiết kế kỹ thuật dự án thành phần hoặc tài liệu vận hành, không thuộc phạm vi Phụ lục I:

- Danh sách cụ thể các cơ sở đào tạo và các nhóm văn bằng, chứng chỉ đưa vào triển khai trong giai đoạn đầu và lộ trình mở rộng theo từng năm;
- Danh sách trường cá nhân loại trừ chi tiết cho từng loại văn bằng, chứng chỉ;
- Lược đồ siêu dữ liệu văn bằng chi tiết (cấu trúc trường, định dạng, quy tắc chuẩn hoá mã);
- Tham số cấu hình chi tiết của Credential Integration Gateway, Credential Hash Engine (kích thước lô, chu kỳ gom, số lần thử lại, TTL của VC trong luồng OIDC4VP);
- Thiết kế chi tiết giao diện Holder Wallet và Verification Portal;
- Quy trình phối hợp nghiệp vụ giữa cơ quan chủ trì sản phẩm, cơ sở đào tạo và các tổ chức tuyển dụng tích hợp Employer Integration API;
- Chính sách phí xác minh (nếu có) đối với các tổ chức tuyển dụng tích hợp API.

SP3 - Bản sao số đô thị (Digital Twin) tích hợp blockchain

1. Định vị sản phẩm

SP3 thuộc Tầng 2 của Đề án, triển khai trong giai đoạn 2028 - 2030 khi các điều kiện dữ liệu, tích hợp, pháp lý và tổ chức thực hiện đã sẵn sàng. Sản phẩm là lớp bằng chứng blockchain tích hợp với nền tảng Digital Twin đô thị của thành phố, ghi nhận bằng chứng đối với các sự kiện hạ tầng có ý nghĩa quản lý: nghiệm thu công trình, cập nhật phiên bản mô hình 3D, bảo trì định kỳ, sửa chữa ngoài kế hoạch, sự cố, dừng vận hành, đưa vào vận hành.

Vai trò đặc trưng của SP3 là "**lớp lọc sự kiện**" giữa luồng cảm biến thời gian thực của Digital Twin và DNC-Chain. Nền tảng Digital Twin tiếp tục quản lý mô hình 3D, dữ liệu cảm biến liên tục, trạng thái vận hành tài sản; SP3 chỉ tiếp nhận các sự kiện có ý nghĩa quản lý theo danh mục allowlist và ghi bằng chứng lên chuỗi. SP3 không xây mới nền tảng Digital Twin, không đưa dữ liệu cảm biến thô liên tục hoặc nội dung mô hình 3D lên chuỗi; chỉ giá trị băm 32 byte của phiên bản mô hình và siêu dữ liệu sự kiện tối thiểu được ghi nhận. Căn cứ thực hiện gồm Luật Xây dựng, Luật Quản lý, sử dụng tài sản công và các quy định chuyên ngành về mô hình thông tin công trình (BIM), mô hình đô thị.

2. Chức năng nghiệp vụ chính

SP3 cung cấp sáu nhóm chức năng:

- Ghi bằng chứng sự kiện hạ tầng có ý nghĩa quản lý theo chuỗi vòng đời tài sản (nghiệm thu, bảo trì, sửa chữa, sự cố, dừng vận hành, đưa vào vận hành);
- Ghi giá trị băm phiên bản mô hình 3D và khối dữ liệu nghiệm thu, hình thành dòng phiên bản tài sản có thể kiểm chứng;

- Thực thi cơ chế đa chữ ký cho sự kiện nghiệm thu hạ tầng (chủ đầu tư, nhà thầu, cơ quan giám sát, đơn vị vận hành);
- Lọc sự kiện giữa luồng cảm biến liên tục và DNC-Chain, loại 100% sự kiện ngoài allowlist;
- Cung cấp giao diện theo dõi lịch sử sự kiện hạ tầng theo dòng thời gian cho chủ đầu tư, ban quản lý dự án và cơ quan giám sát;
- Kiểm chứng độc lập khi có tranh chấp về chất lượng công trình, tình trạng bảo trì hoặc thời điểm phát sinh sự cố.

3. Kiến trúc kỹ thuật đặc thù

SP3 tổ chức theo kiến trúc hai lớp: lớp off-chain đóng vai trò lọc và chuẩn hoá sự kiện giữa nền tảng Digital Twin và DNC-Chain; lớp on-chain gồm ba hợp đồng thông minh riêng trên DNC-Chain.

Bảng C.4.1. Cấu phần off-chain và on-chain của SP3

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Digital Twin Event Listener	Tiếp nhận sự kiện từ nền tảng Digital Twin qua OGC SensorThings API; lọc sự kiện theo allowlist; loại bỏ luồng cảm biến liên tục
Off-chain	Infrastructure Event Standardization Engine	Chuẩn hoá sự kiện theo ISO 19650 (BIM), CityGML 3.0, IFC; gán mã tài sản hạ tầng theo quy chuẩn quản lý tài sản công
Off-chain	Model Version Hash Service	Tính SHA-256 của phiên bản mô hình 3D hoặc khối dữ liệu nghiệm thu; không lưu nội dung mô hình lên chuỗi
Off-chain	Multi-Signature Orchestrator	Điều phối quy trình đa chữ ký cho sự kiện nghiệm thu (chủ đầu tư, nhà thầu, giám sát, vận hành)
Off-chain	Infrastructure Dashboard	Giao diện theo dõi lịch sử sự kiện hạ tầng theo dòng thời gian; phục vụ chủ đầu tư, ban quản lý, cơ quan giám sát
Off-chain	Oracle Gateway	Giao diện chuẩn hoá tiếp nhận dữ liệu ngoài (thời tiết, giao thông, năng lượng) khi cần kiểm chứng; kế thừa OracleInterfaceTemplate của Mô đun 5
On-chain	InfraEventRegistry	Hợp đồng thông minh riêng; ghi bằng chứng sự kiện hạ tầng có ý nghĩa quản lý; kế thừa ProofRegistryTemplate của Mô đun 5

Lớp	Cấu phần	Chức năng kỹ thuật chính
On-chain	ModelVersionRegistry	Hợp đồng thông minh riêng; ghi giá trị băm phiên bản mô hình 3D và khôi dữ liệu nghiệm thu
On-chain	AcceptanceMultiSig	Hợp đồng thông minh riêng; thực thi đa chữ ký cho nghiệm thu; kế thừa MultiSignatureTemplate của Mô đun 5

Ba hợp đồng thông minh riêng tuân thủ EIP-712, ERC-165, OpenZeppelin Governor và Gnosis Safe compatible. Cấu trúc dữ liệu sự kiện trên InfraEventRegistry gồm các trường kỹ thuật (eventId, assetIdHash, eventTypeCode, modelVersionId, actorRefList, timestamp, geoHash với độ chính xác $20m \times 20m$ đủ để định vị tài sản hạ tầng nhưng không định vị cá nhân, metadataURI, statusCode); trên ModelVersionRegistry lưu modelVersionId, assetIdHash, modelHash, modelStandard (ISO 19650 / CityGML 3.0 / IFC), previousVersionId (tạo dòng phiên bản). Danh sách trường loại trừ không được ghi lên chuỗi gồm: dữ liệu cảm biến thô liên tục (nhiệt độ, độ ẩm, độ rung, lưu lượng giao thông theo từng giây); nội dung toàn văn mô hình 3D, tệp IFC, CityGML, BIM; hình ảnh camera giám sát đô thị, hình ảnh vệ tinh chi tiết; hồ sơ thiết kế chi tiết, bản vẽ thi công, dự toán, hợp đồng xây dựng; thông tin cá nhân kỹ sư, công nhân, cán bộ giám sát; dữ liệu thương mại nhạy cảm của nhà thầu; tọa độ GPS chính xác của cá nhân.

Luồng kỹ thuật cơ bản: khi nền tảng Digital Twin cập nhật phiên bản mô hình hoặc phát sinh sự kiện hạ tầng (bảo trì, sửa chữa, sự cố), Digital Twin Event Listener nhận qua OGC SensorThings API và kiểm tra allowlist. Model Version Hash Service tính SHA-256 của khối dữ liệu mô hình, gắn dấu thời gian RFC 3161. ModelVersionRegistry ghi giá trị băm và liên kết với phiên bản trước qua trường previousVersionId; InfraEventRegistry ghi sự kiện tương ứng. Đối với nghiệm thu hạ tầng, quy trình đa chữ ký được kích hoạt: chủ đầu tư khởi tạo đề xuất qua Multi-Signature Orchestrator với modelVersionId và biên bản nghiệm thu (lưu off-chain); AcceptanceMultiSig gọi proposeAcceptance() chuyển trạng thái sang "chờ phê duyệt"; nhà thầu, cơ quan giám sát và đơn vị vận hành lần lượt ký số phê duyệt; khi đủ ngưỡng cấu hình (mặc định 3/4 chữ ký), hợp đồng gọi executeAcceptance() và InfraEventRegistry ghi sự kiện nghiệm thu chính thức. Thời gian chờ tối đa cho quy trình đa chữ ký là 30 ngày; quá hạn đề xuất tự động hủy. Khi có tranh chấp, Infrastructure Dashboard truy xuất chuỗi sự kiện và dòng phiên bản mô hình; Model Version Hash Service tính lại giá trị băm từ mô hình hiện có tại Digital Twin và so sánh với giá trị đã ghi để xác định tính toàn vẹn.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP3: M1: TC; M2: B; M3: B; M4: TC; M5: B; M6: B; M7: TC.

- **Mô đun 2 (bắt buộc):** InfraEventRegistry và ModelVersionRegistry gọi ProofRegistry của Mô đun 2 để ghi bằng chứng; BatchManager được sử dụng khi số sự kiện đồng thời lớn (ví dụ đợt nghiệm thu đồng loạt các hạng mục của một dự án lớn).

- **Mô đun 3 (bắt buộc):** quản lý năm vai trò đặc thù vòng đời hạ tầng: ROLE_PROJECT_OWNER (chủ đầu tư), ROLE_CONTRACTOR (nhà thầu), ROLE_SUPERVISOR (cơ quan giám sát), ROLE_OPERATOR (đơn vị vận hành hạ tầng), ROLE_DT_ADMIN (đơn vị quản trị nền tảng Digital Twin).

- **Mô đun 5 (bắt buộc):** ba hợp đồng thông minh riêng đăng ký vào ContractRegistry; AcceptanceMultiSig kế thừa MultiSignatureTemplate; Oracle Gateway kế thừa OracleInterfaceTemplate. Nâng cấp theo Proxy Upgrade Pattern với đa ký và timelock 48 giờ.

- **Mô đun 6 (bắt buộc):** SP3 đăng ký vào ApplicationRegistry; trạng thái vòng đời quản lý bởi LifecycleManager; công bố trên Marketplace Portal.

Mức tùy chọn Mô đun 4 áp dụng khi cần phát hành token xác nhận nghiệm thu hạ tầng (acceptance certificate token), mặc định không kích hoạt. Mức tùy chọn Mô đun 7 áp dụng cho cán bộ ký số đại diện các bên tham gia đa chữ ký (Hub ID cho cán bộ, không cho tài sản hạ tầng). Mức tùy chọn Mô đun 1 áp dụng khi có nhu cầu phối hợp giám sát liên tỉnh hoặc quốc tế.

SP3.5. Giao diện và tích hợp

SP3 tích hợp với nền tảng Digital Twin đô thị của thành phố (đã có hoặc đang xây dựng) và năm nhóm hệ thống nghiệp vụ của các bên tham gia vòng đời hạ tầng: nền tảng Digital Twin (sự kiện cập nhật mô hình, cập nhật trạng thái tài sản); hệ thống quản lý dự án đầu tư công (sự kiện khởi công, nghiệm thu theo giai đoạn, hoàn thành); hệ thống quản lý tài sản công (mã tài sản, thông tin tổng hợp); hệ thống quản lý bảo trì hạ tầng (sự kiện bảo trì, sửa chữa, thay thế thiết bị); hệ thống giám sát của cơ quan có thẩm quyền (sự kiện giám sát chất lượng công trình).

Bảng C.4.2. Giao diện kỹ thuật chính của SP3

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Nền tảng Digital Twin đô thị	REST/WebSocket theo OGC SensorThings API	mTLS + JWT + ROLE_DT_ADMIN
Hệ thống quản lý dự án, quản lý tài sản, bảo trì	REST trên HTTPS qua LGSP	mTLS + JWT + chữ ký số của cơ quan vận hành hệ thống
Chủ đầu tư, nhà thầu, giám sát, vận hành (các bên tham gia đa chữ ký)	Multi-Signature Orchestrator; Infrastructure Dashboard	JWT + vai trò tương ứng ROLE_PROJECT_OWNER/CONTRACTOR/SUPERVISOR/OPERATOR
Cơ quan thanh tra, hậu kiểm	Infrastructure Dashboard (quyền xem và xuất báo cáo)	mTLS + JWT + ROLE_AUDITOR
Nguồn dữ liệu ngoài (thời tiết, giao thông, năng lượng)	Oracle Gateway theo AggregatorV3Interface	Theo đặc tả OracleInterfaceTemplate tại Phần B Mục 5

Chuẩn kỹ thuật cốt lõi: ISO 19650 và Industry Foundation Classes (IFC) cho mô hình thông tin công trình; CityGML 3.0 cho mô hình đô thị; OGC SensorThings API cho giao diện cảm biến; Geohash 8 ký tự (độ chính xác $20\text{m} \times 20\text{m}$) cho định vị địa lý tài sản (không sử dụng tọa độ GPS chính xác). Các chuẩn mật mã chung (ECDSA secp256k1, SHA-256, keccak256, RFC 3161) và cơ chế đa chữ ký (OpenZeppelin Governor, Gnosis Safe compatible) áp dụng theo quy định chung tại Phần A Mục VII và Phần B Mục 5.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.4.3. Chỉ tiêu mức dịch vụ cốt lõi của SP3

Chỉ tiêu	Mức cam kết
Thời gian ghi sự kiện hạ tầng từ khi nhận từ Digital Twin	≤ 60 giây với 99% sự kiện tính theo tháng
Thời gian ghi phiên bản mô hình từ khi cập nhật	≤ 2 phút với 99% phiên bản tính theo tháng
Thời gian hoàn thành nghiệm thu qua đa chữ ký	Trung bình ≤ 15 ngày khi có đủ điều kiện; tối đa 30 ngày
Thời gian tra cứu tại Infrastructure Dashboard	≤ 3 giây với 99% lượt tính theo tháng
Tỷ lệ lọc đúng sự kiện có ý nghĩa quản lý (không đưa cảm biến liên tục lên chuỗi)	100% sự kiện ngoài allowlist bị loại trừ
Tỷ lệ ghi sự kiện thành công	$\geq 99,9\%$ tính theo tháng

Chỉ tiêu thời gian phục hồi sau sự cố ($\text{RTO} \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($\text{RPO} \leq 15$ phút) áp dụng theo quy định chung tại Phần A Mục VII. Chỉ tiêu "lọc đúng 100% sự kiện ngoài allowlist" là chỉ tiêu đặc thù của SP3, được kiểm chuẩn độc lập do bản chất "lớp lọc sự kiện" là vai trò chính của sản phẩm này.

7. Điều kiện triển khai và giới hạn phạm vi

Điều kiện kỹ thuật triển khai SP3:

- Nền tảng Digital Twin đô thị của thành phố đã vận hành với giao diện OGC SensorThings API hoặc tương đương;

- Hệ thống quản lý tài sản công đã cấp mã tài sản thống nhất cho các hạ tầng trong phạm vi triển khai;
- Chủ đầu tư, nhà thầu, cơ quan giám sát, đơn vị vận hành đã đăng ký khóa ký số vào KeyRegistry của Mô đun 3; mỗi bên đã được cấp vai trò tương ứng trong AccessControlRegistry;
- Quy trình đa chữ ký nghiệm thu đã được cơ quan có thẩm quyền ban hành kèm ngưỡng chữ ký và thời gian chờ cho từng loại công trình;
- Allowlist sự kiện được ghi lên chuỗi đã được cơ quan chủ trì sản phẩm phê duyệt bằng văn bản;
- Ba hợp đồng InfraEventRegistry, ModelVersionRegistry, AcceptanceMultiSig đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;
- SP3 đã được đăng ký vào ApplicationRegistry của Mô đun 6 và chuyển sang trạng thái vận hành chính thức;
- Kết quả triển khai Tầng 1 đã được đánh giá đủ cơ sở chuyển sang Tầng 2 theo lộ trình tại Bảng 3 Mục IV Chương III của Đề án.

Giới hạn phạm vi đặc tả của Phụ lục đối với SP3. Các nội dung sau thuộc hồ sơ thiết kế kỹ thuật dự án thành phần hoặc tài liệu vận hành, không thuộc phạm vi Phụ lục I:

- Danh sách cụ thể các hạng mục hạ tầng đưa vào triển khai trong giai đoạn đầu và lộ trình mở rộng theo từng năm;
- Allowlist sự kiện chi tiết cho từng nhóm tài sản hạ tầng (tòa nhà công, hạ tầng giao thông, hạ tầng cấp thoát nước, hạ tầng năng lượng, công viên cây xanh, trường học, bệnh viện);
- Ngưỡng đa chữ ký cụ thể cho từng loại công trình (công trình cấp đặc biệt, cấp I, cấp II, cấp III);
- Tham số cấu hình chi tiết (chu kỳ gom, ngưỡng lọc cảm biến, số lần thử lại);
- Thiết kế chi tiết giao diện Infrastructure Dashboard;
- Quy trình phối hợp giữa đơn vị quản trị nền tảng Digital Twin với các cơ quan chuyên ngành về quản lý đô thị, xây dựng, giao thông;
- Danh mục nguồn dữ liệu ngoài được tích hợp qua Oracle Gateway và quy trình phê duyệt bổ sung nguồn mới.

SP4 - Hệ thống xác minh hồ sơ y tế trên blockchain

1. Định vị sản phẩm

SP4 thuộc Tầng 2 của Đề án, triển khai trong giai đoạn 2028 - 2030 khi các điều kiện dữ liệu, pháp lý chuyên ngành y tế, cơ chế phối hợp liên ngành và tổ chức thực hiện đã sẵn sàng. Sản phẩm là nền tảng ghi nhận bằng chứng đối với các sự kiện y tế có ý nghĩa quản lý và phát hành Chứng nhận xác minh sự kiện y tế dưới dạng Verifiable Credential (VC) cho người bệnh.

SP4 có yêu cầu bảo vệ dữ liệu cá nhân ở mức cao nhất trong 10 sản phẩm do dữ liệu y tế thuộc nhóm dữ liệu cá nhân nhạy cảm theo Điều 3 Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15. SP4 không ghi nội dung hồ sơ y tế, không ghi chẩn đoán, đơn thuốc, kết quả xét nghiệm, dữ liệu cá nhân chi tiết lên chuỗi trong mọi trường hợp; chỉ ghi bằng chứng mật mã của các sự kiện y tế có ý nghĩa quản lý (tiếp nhận bệnh nhân, hoàn tất điều trị, chuyển viện, thanh toán bảo hiểm y tế, cấp giấy khám sức khỏe, cấp giấy chứng sinh, cấp giấy chứng tử) với siêu dữ liệu kỹ thuật tối thiểu. Căn cứ thực hiện: Luật Khám bệnh, chữa bệnh số 15/2023/QH15, Luật Bảo hiểm y tế, Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và các quy định chuyên ngành của Bộ Y tế.

2. Chức năng nghiệp vụ chính

SP4 cung cấp sáu nhóm chức năng:

- Ghi bằng chứng sự kiện y tế có ý nghĩa quản lý khi phát sinh tại hệ thống quản lý bệnh viện (HIS);
- Phát hành Chứng nhận xác minh sự kiện y tế theo W3C VC Data Model **v2.0** cho người bệnh;
- Quản lý quyền đồng ý chia sẻ của người bệnh theo phạm vi, thời hạn và mục đích, có hỗ trợ rút quyền bất cứ lúc nào (cơ chế Consent-based Access);
- Xác minh sự kiện y tế theo yêu cầu (cơ sở y tế khác, tổ chức bảo hiểm) với điều kiện người bệnh đã đồng ý;
- Hỗ trợ chuyển viện có kiểm soát với đồng ý của người bệnh;
- Phát hiện mẫu kê khai bất thường phục vụ giám sát bảo hiểm y tế, trên dữ liệu tổng hợp ẩn danh, không truy cập bệnh án chi tiết.

3. Kiến trúc kỹ thuật đặc thù

SP4 tổ chức theo kiến trúc hai lớp: lớp off-chain đặt tại hạ tầng dữ liệu của cơ sở khám, chữa bệnh và của ngành y tế thành phố, đóng vai trò "công kiểm soát" chặt chẽ trước khi bất kỳ dữ liệu nào được đưa lên chuỗi; lớp on-chain gồm ba hợp đồng thông minh riêng trên DNC-Chain.

Bảng C.5.1. Cấu phần off-chain và on-chain của SP4

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	HIS Integration Gateway	Tiếp nhận sự kiện y tế từ HIS qua LGSP; xác minh cơ sở y tế; tuyệt đối không chuyển nội dung hồ sơ y tế, chẩn đoán, đơn thuốc, kết quả xét nghiệm sang các cấu phần phía sau
Off-chain	Medical Event Filter	Lọc sự kiện theo allowlist sự kiện có ý nghĩa quản lý; từ chối tuyệt đối sự kiện không thuộc allowlist

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Medical Event Standardization Engine	Chuẩn hoá theo HL7 FHIR R4, chỉ sử dụng Resource Encounter, EpisodeOfCare, Consent; không sử dụng các Resource chứa dữ liệu lâm sàng chi tiết
Off-chain	Hub ID Resolver	Chuyển mã bệnh nhân sang Hub ID qua Mô đun 7; ánh xạ lưu tại hệ thống nguồn, không tại SP4
Off-chain	VC Issuance Service	Phát hành Chứng nhận xác minh theo W3C VC Data Model v2.0; ký số bằng khóa riêng cơ sở y tế
Off-chain	Patient Wallet	Ví định danh số cho người bệnh; lưu và xuất trình VC; hỗ trợ Selective Disclosure và cấp quyền chia sẻ
Off-chain	Aggregated Analytics Engine	Phân tích sự kiện tổng hợp ẩn danh; không truy cập bệnh án chi tiết
Off-chain	Payer Verification API	Giao diện cho tổ chức bảo hiểm, tổ chức có nhu cầu xác minh sự kiện y tế
On-chain	MedEventRegistry	Hợp đồng thông minh riêng; ghi bằng chứng sự kiện y tế; kế thừa ProofRegistryTemplate của Mô đun 5
On-chain	MedEventRevocationList	Hợp đồng thông minh riêng; danh sách sự kiện y tế đã bị thu hồi hoặc điều chỉnh
On-chain	ConsentRegistry	Hợp đồng thông minh riêng; quản lý quyền đồng ý chia sẻ của người bệnh theo phạm vi, thời hạn, mục đích

Ba hợp đồng thông minh riêng tuân thủ EIP-712, ERC-165, W3C Status List 2021, RFC 5280, W3C VC Data Model v2.0. Cấu trúc dữ liệu sự kiện y tế trên MedEventRegistry gồm các trường kỹ thuật (eventId, patientHubId do Mô đun 7 cấp, issuerDID cơ sở y tế, eventTypeCode, eventRefHash mã sự kiện HIS đã băm, timestamp, metadataURI chỉ chứa mã chuyên khoa và loại hình cơ sở - không chứa chẩn đoán, đơn thuốc, kết quả xét nghiệm); ConsentRegistry lưu consentId, patientHubId, grantedToDID bên được chia sẻ, scopeHash (chỉ băm, phạm vi chi tiết lưu off-chain), purposeCode, expiresAt, statusCode. Danh sách trường loại trừ - áp dụng ở mức cao nhất trong 10 sản phẩm - không được ghi lên chuỗi gồm: họ tên, số định danh cá nhân, ngày sinh, giới tính, địa chỉ, số điện thoại, địa chỉ thư điện tử của người bệnh; chẩn đoán dưới mọi dạng (mã ICD-10, ICD-11, mô tả chẩn đoán, chẩn đoán sơ bộ, chẩn đoán phân biệt); đơn thuốc,

danh mục thuốc, liều dùng; kết quả xét nghiệm, chẩn đoán hình ảnh, giải phẫu bệnh; tiền sử bệnh, tiền sử dị ứng, tiền sử gia đình; dữ liệu sinh trắc học, di truyền, sức khỏe sinh sản; thông tin quan hệ tình dục, chất gây nghiện, sức khỏe tâm thần; hình ảnh y tế; nội dung toàn văn bệnh án điện tử; danh tính bác sĩ, điều dưỡng, nhân viên y tế phụ trách ca bệnh; chi phí điều trị chi tiết, phương thức thanh toán, mã thẻ bảo hiểm y tế.

Luồng kỹ thuật cơ bản: khi HIS phát sinh sự kiện y tế, dữ liệu được chuyển qua LGSP đến HIS Integration Gateway. Gateway xác minh cơ sở y tế qua IssuerWhitelist của Mô đun 7 và IssuerRegistry của Mô đun 2, loại tuyệt đối các trường thuộc danh sách loại trừ. Medical Event Filter kiểm tra sự kiện thuộc allowlist, từ chối nếu không thuộc. Medical Event Standardization Engine chuẩn hoá theo HL7 FHIR R4 (chỉ Resource Encounter, EpisodeOfCare). Hub ID Resolver chuyển mã bệnh nhân sang Hub ID qua Mô đun 7 (ánh xạ lưu tại hệ thống nguồn, không tại SP4). MedEventRegistry gọi BatchManager của Mô đun 2 ghi bằng chứng theo cơ chế gom lô; VC Issuance Service phát hành VC đăng ký vào VCRegistry của Mô đun 7; người bệnh tiếp nhận VC vào Patient Wallet. Khi có yêu cầu xác minh, người bệnh cấp quyền đồng ý qua grantConsent() của ConsentRegistry với phạm vi, thời hạn và mục đích cụ thể; sau đó xuất trình VC qua luồng OIDC4VP của Mô đun 7. Bên xác minh gọi Verification API của Mô đun 7, hệ thống kiểm tra tính hiệu lực của quyền đồng ý qua checkConsentValidity() và kiểm chứng chữ ký số cơ sở y tế phát hành. Khi người bệnh rút quyền qua revokeConsent(), ConsentRegistry cập nhật trạng thái "đã rút quyền"; Mô đun 7 cập nhật VCRevocationList đối với các VC liên quan. Trong trường hợp chuyển viện, dữ liệu lâm sàng được chuyển qua mạng chuyên dùng của ngành y tế, không đi qua DNC-Chain; DNC-Chain chỉ ghi sự kiện "chuyển viện đi" tại cơ sở chuyển và "chuyển viện đến" tại cơ sở tiếp nhận.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP4: M1: TC; **M2: BB**; M3: B; M4: TC; M5: B; M6: B; **M7: BB**.

- **Mô đun 2 (bắt buộc cốt lõi):** MedEventRegistry gọi ProofRegistry và BatchManager của Mô đun 2 để ghi bằng chứng theo cơ chế gom lô. Yêu cầu uptime cao do tính cấp thiết của ghi nhận sự kiện y tế (chuyển viện, cấp cứu).

- **Mô đun 7 (bắt buộc cốt lõi):** người bệnh định danh bằng Hub ID, không dùng họ tên, số định danh cá nhân trên chuỗi. Các VC y tế đăng ký vào VCRegistry; cơ sở y tế đăng ký vào IssuerWhitelist. Mô đun 7 cung cấp các cơ chế tăng cường bảo vệ quyền riêng tư (Selective Disclosure, BBS+ Signatures, Zero-Knowledge Proof tùy chọn) đặc biệt có ý nghĩa với SP4.

- **Mô đun 3 (bắt buộc):** quản lý các vai trò ROLE_MED_ISSUER (cơ sở khám, chữa bệnh được ủy quyền), ROLE_MED_REVOKER (cơ sở y tế được thu hồi, điều chỉnh sự kiện), ROLE_PAYER_VERIFIER (tổ chức bảo hiểm), ROLE_MED_AUDITOR (cơ quan quản lý y tế, Bảo hiểm xã hội, Thanh tra y tế).

- **Mô đun 5 (bắt buộc):** ba hợp đồng đăng ký vào ContractRegistry; nâng cấp theo Proxy Upgrade Pattern với đa ký và timelock 48 giờ.

- **Mô đun 6 (bắt buộc):** SP4 đăng ký vào ApplicationRegistry; AccessGate của Mô đun 6 kiểm soát truy cập cấp ứng dụng đối với Payer Verification API.

Mức tùy chọn Mô đun 4 không kích hoạt mặc định; chỉ xem xét khi có yêu cầu đặc thù về phát hành chứng nhận năng lực hành nghề, chứng chỉ hành nghề y tế theo cơ chế riêng. Mức tùy chọn Mô đun 1 chỉ kích hoạt khi được cơ quan có thẩm quyền phê duyệt và người bệnh đã đồng ý.

5. Giao diện và tích hợp

SP4 tích hợp với năm nhóm hệ thống nguồn: hệ thống HIS của bệnh viện công lập (tuyến thành phố, tuyến quận huyện); hệ thống HIS của cơ sở khám, chữa bệnh ngoài công lập tham gia thí điểm; hệ thống của trạm y tế và trung tâm y tế phường, xã (sự kiện khám ban đầu, cấp giấy chứng sinh, cấp giấy khám sức khỏe); hệ thống giám định bảo hiểm y tế (sự kiện thanh toán bảo hiểm); trong giai đoạn mở rộng có thể kết nối với Hệ thống hồ sơ sức khỏe điện tử toàn dân do Bộ Y tế chủ trì. Tích hợp thực hiện qua LGSP theo Nghị định số 278/2025/NĐ-CP và qua mạng chuyên dùng của ngành y tế theo quy định chuyên ngành.

Bảng C.5.2. Giao diện kỹ thuật chính của SP4

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Hệ thống HIS qua LGSP	REST trên HTTPS; webhook nhận biên lai	mTLS + JWT + chữ ký số ERC-191 của cơ sở y tế
Hệ thống ngành y tế qua mạng chuyên dùng	Theo quy định của Bộ Y tế; HL7 FHIR R4	mTLS + chứng thư số ngành y tế
Người bệnh	Patient Wallet; luồng OIDC4VP khi xuất trình VC	Khóa riêng của người bệnh
Tổ chức bảo hiểm, cơ sở y tế khác	Payer Verification API; Verification API của Mô đun 7	JWT + ROLE_PAYER_VERIFIER (với tổ chức bảo hiểm); xác minh đồng thời quyền đồng ý từ ConsentRegistry
Cơ quan quản lý y tế, Bảo hiểm xã hội, Thanh tra y tế	Aggregated Analytics Engine; giao diện quản trị	mTLS + JWT + ROLE_MED_AUDITOR

Chuẩn kỹ thuật cốt lõi: HL7 FHIR R4 (chỉ Resource Encounter, EpisodeOfCare, Consent); không sử dụng mã chẩn đoán ICD trực tiếp trên chuỗi; W3C DID Core v1.0 và Hub ID của Mô đun 7 cho định danh người bệnh từ VNeID; W3C VC Data Model **v2.0** cho Chứng nhận xác minh và VC Consent; OIDC4VP và OIDC4VCI qua Mô đun 7. HSM của cơ sở y tế đạt quy chuẩn tương đương FIPS 140-3 Level 3 theo yêu cầu tại Phần A Mục VII, ưu tiên thiết bị trong nước đã được Ban Cơ yếu Chính phủ chứng nhận. AES-256 cho mã hoá siêu dữ liệu off-chain có mức nhạy cảm. Các chuẩn mật mã chung

(ECDSA secp256k1, SHA-256, keccak256, RFC 3161) áp dụng theo quy định tại Phần A Mục VII.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.5.3. Chỉ tiêu mức dịch vụ cốt lõi của SP4

Chỉ tiêu	Mức cam kết
Thời gian ghi bằng chứng sự kiện y tế từ khi HIS phát sinh	≤ 90 giây với 99% sự kiện tính theo tháng
Thời gian xác minh qua OIDC4VP	≤ 5 giây với 99% lượt tính theo tháng
Thời gian cấp quyền đồng ý trên Patient Wallet (ConsentGranted)	≤ 2 giây
Tỷ lệ ghi bằng chứng thành công	$\geq 99,9\%$ tính theo tháng
Tỷ lệ lọc đúng sự kiện theo allowlist (không đưa dữ liệu ngoài allowlist)	100% sự kiện ngoài allowlist bị từ chối
Tỷ lệ loại trừ đúng trường cấm (không đưa dữ liệu trong danh sách loại trừ)	100% trường loại trừ bị loại khỏi luồng

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút) áp dụng theo quy định chung tại Phần A Mục VII. Hai chỉ tiêu "lọc đúng 100% sự kiện ngoài allowlist" và "loại trừ đúng 100% trường cấm" là chỉ tiêu đặc thù quan trọng nhất của SP4, được kiểm chuẩn độc lập trước khi vận hành và định kỳ trong quá trình vận hành, do tính nhạy cảm của dữ liệu y tế.

7. Điều kiện triển khai và giới hạn phạm vi

Điều kiện kỹ thuật triển khai SP4:

- Hệ thống HIS của cơ sở khám, chữa bệnh tham gia đã hỗ trợ trao đổi dữ liệu theo HL7 FHIR R4 ở mức Resource Encounter, EpisodeOfCare, Consent;
- Cơ sở khám, chữa bệnh đã đăng ký vào IssuerWhitelist của Mô đun 7 và IssuerRegistry của Mô đun 2 với phạm vi loại sự kiện được phép phát hành VC, có phê duyệt bằng văn bản;
- Khóa ký số cơ sở y tế đã đăng ký vào KeyRegistry của Mô đun 3; HSM đạt quy chuẩn tương đương FIPS 140-3 Level 3;
- LGSP đã cấp kênh mTLS đến HIS Integration Gateway;

- Cơ quan chủ trì sản phẩm đã ban hành allowlist sự kiện và danh sách trường loại trừ, có phê duyệt của Sở Y tế;

- Quy trình cấp quyền đồng ý và rút quyền đồng ý của người bệnh đã được ban hành, bao gồm quy định riêng đối với người bệnh chưa có năng lực hành vi dân sự đầy đủ (người chưa thành niên, người mất năng lực hành vi dân sự);

- Ba hợp đồng MedEventRegistry, MedEventRevocationList, ConsentRegistry đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII; kiểm toán có nội dung chuyên biệt về bảo vệ dữ liệu cá nhân y tế do đơn vị kiểm toán có chuyên môn bảo vệ dữ liệu cá nhân nhạy cảm thực hiện;

- Đã xin ý kiến Bộ Y tế về khả năng kết nối với Hệ thống hồ sơ sức khỏe điện tử toàn dân trong giai đoạn mở rộng;

- Kết quả triển khai Tầng 1 đã được đánh giá đủ cơ sở chuyển sang Tầng 2 theo lộ trình tại Bảng 3 Mục IV Chương III của Đề án;

- SP4 đã được đăng ký vào ApplicationRegistry của Mô đun 6 và chuyển sang trạng thái vận hành chính thức.

Giới hạn phạm vi đặc tả của Phụ lục đối với SP4. Các nội dung sau thuộc hồ sơ thiết kế kỹ thuật dự án thành phần hoặc tài liệu vận hành, không thuộc phạm vi Phụ lục I:

- Danh sách cụ thể các cơ sở khám, chữa bệnh và các nhóm sự kiện y tế đưa vào triển khai trong giai đoạn đầu và lộ trình mở rộng theo từng năm;

- Allowlist sự kiện y tế chi tiết và danh sách trường loại trừ chi tiết (do cơ quan chủ trì sản phẩm ban hành, có phê duyệt của Sở Y tế);

- Lược đồ HL7 FHIR R4 chi tiết áp dụng cho từng loại sự kiện;

- Tham số cấu hình chi tiết (kích thước lô gom bằng chứng y tế, chu kỳ, TTL của VC trong OIDC4VP, ngưỡng phân tích tổng hợp tối thiểu, thời hạn mặc định quyền đồng ý);

- Thiết kế chi tiết giao diện Patient Wallet;

- Quy trình cấp quyền đồng ý và rút quyền đồng ý của người bệnh (đặc biệt đối với người chưa có năng lực hành vi dân sự đầy đủ);

- Cơ chế xử lý tình huống khẩn cấp (cấp cứu, người bệnh không có khả năng cấp quyền đồng ý ngay lập tức);

- Quy định về trách nhiệm của cơ sở y tế khi thu hồi hoặc điều chỉnh sự kiện y tế đã ghi trên chuỗi;

- Cơ chế phối hợp giữa SP4 với Hệ thống hồ sơ sức khỏe điện tử toàn dân của Bộ Y tế (khi kết nối mở rộng).

SP5 - Sàn giao dịch dữ liệu thành phố tích hợp blockchain

1. Định vị sản phẩm

SP5 thuộc Tầng 3 của Đề án, triển khai trong giai đoạn 2028 - 2030. Sản phẩm là nền tảng niêm yết dữ liệu, cấp phép khai thác, ghi nhận quyền truy cập và giám sát khai thác dữ liệu trên địa bàn thành phố. Nguyên tắc kỹ thuật xuyên suốt SP5 là "dữ liệu gốc không ghi lên chuỗi": blockchain chỉ ghi giá trị băm của hồ sơ niêm yết, mã tham chiếu giấy phép, các mốc cấp phép và nhật ký truy vấn tổng hợp; toàn bộ dữ liệu gốc vẫn do chủ sở hữu dữ liệu quản lý tại hệ thống nguồn.

Phạm vi áp dụng tuân thủ Luật Dữ liệu số 60/2024/QH15 và Nghị định số 278/2025/NĐ-CP. SP5 không áp dụng đối với dữ liệu thuộc Danh mục dữ liệu quan trọng, dữ liệu cốt lõi theo Quyết định số 20/2025/QĐ-TTg; dữ liệu thuộc danh mục này chỉ được đưa vào SP5 khi có quyết định cho phép của cơ quan có thẩm quyền. Dữ liệu có chứa dữ liệu cá nhân phải tuân thủ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP.

2. Chức năng nghiệp vụ chính

SP5 cung cấp sáu nhóm chức năng:

- Niêm yết dữ liệu và dịch vụ dữ liệu với siêu dữ liệu, điều kiện khai thác, phạm vi, thời hạn, giá;
- Phân loại dữ liệu và đánh giá nguy cơ tái định danh theo ba mức (thấp, trung bình, cao);
- Cấp phép khai thác dữ liệu qua Token định danh giấy phép không chuyển nhượng (LicenseSBT);
- Kiểm soát truy cập dữ liệu hoặc API khai thác theo phạm vi cấp phép (hạn mức truy vấn, khối lượng kết xuất);
- Giám sát nguy cơ tái định danh và phát hiện truy vấn bất thường, áp dụng làm tròn, ẩn bớt thuộc tính, giới hạn kết quả truy vấn;
- Thu hồi hoặc chấm dứt giấy phép khi có vi phạm hoặc yêu cầu của cơ quan có thẩm quyền.

3. Kiến trúc kỹ thuật đặc thù

SP5 tổ chức theo kiến trúc hai lớp: lớp off-chain đặt tại hạ tầng dữ liệu của thành phố và hệ thống của chủ sở hữu dữ liệu; lớp on-chain gồm bốn hợp đồng thông minh riêng trên DNC-Chain.

Bảng C.6.1. Cấu phần off-chain và on-chain của SP5

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Data Listing Portal	Công niêm yết bộ dữ liệu và dịch vụ dữ liệu

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Data Classification and Risk Engine	Phân loại dữ liệu, đánh giá mức nhạy cảm, đánh giá nguy cơ tái định danh; kiểm tra dữ liệu có thuộc Quyết định số 20/2025/QĐ-TTg
Off-chain	Listing Hash Service	Tính SHA-256 của hồ sơ niêm yết; ký số chủ sở hữu dữ liệu
Off-chain	License Management Service	Tiếp nhận yêu cầu cấp phép; phê duyệt; quản lý phạm vi, thời hạn, mục đích, gia hạn, điều chỉnh, thu hồi
Off-chain	Access Control Gateway	Kiểm soát truy cập dữ liệu đúng phạm vi cấp phép; giới hạn truy vấn, khối lượng, kết xuất
Off-chain	Re-identification Risk Control Service	Giám sát nguy cơ tái định danh; áp dụng làm tròn, ẩn bớt thuộc tính, giới hạn kết quả, cảnh báo và ngắt quyền khi vượt ngưỡng
Off-chain	Audit Trail Service	Ghi nhật ký truy cập, khai thác, sự kiện giao dịch, dấu hiệu truy vấn bất thường
Off-chain	Data Service and Marketplace Portal	Kết nối cung cầu khai thác dữ liệu; dịch vụ giá trị gia tăng
On-chain	DataListingRegistry	Hợp đồng thông minh riêng; ghi giá trị băm hồ sơ niêm yết; kế thừa ProofRegistryTemplate của Mô đun 5
On-chain	DataLicenseRegistry	Hợp đồng thông minh riêng; quản lý vòng đời giấy phép (cấp mới, gia hạn, điều chỉnh, thu hồi)
On-chain	DataAccessLog	Hợp đồng thông minh riêng; ghi mã tham chiếu các phiên khai thác và cảnh báo bất thường
On-chain	LicenseSBT	Hợp đồng thông minh riêng; đúc Token định danh giấy phép không chuyển nhượng gắn Hub ID bên khai thác theo ERC-721 với transferable=false

Bốn hợp đồng thông minh riêng tuân thủ EIP-712, ERC-165 và ERC-721 (với thuộc tính transferable=false cho LicenseSBT). Cấu trúc dữ liệu niêm yết trên DataListingRegistry gồm các trường kỹ thuật (listingId, ownerDID, listingHash, classificationCode 3 mức phân loại, riskLevelCode 3 mức nguy cơ tái định danh,

metadataURI, statusCode); DataLicenseRegistry lưu licenseId, listingId, consumerHubId, scopeHash, purposeCode, startAt, expiresAt, statusCode, priceRefHash (chỉ băm tham chiếu, giá cụ thể lưu off-chain), licenseSBTTOKENId. Danh sách trường loại trừ không được ghi lên chuỗi gồm: nội dung dữ liệu gốc (toàn bộ dữ liệu và từng bản ghi); trường có khả năng tái định danh cá nhân (họ tên, số định danh, ngày sinh, địa chỉ, số điện thoại, dữ liệu sinh trắc học, dữ liệu vị trí chi tiết); kết quả truy vấn chi tiết, phản hồi API, nội dung tập tin tải xuống; danh mục khách hàng, đối tác của bên khai thác; giá cụ thể giao dịch dữ liệu; nội dung hợp đồng chi tiết; dữ liệu thuộc Danh mục dữ liệu quan trọng, dữ liệu cốt lõi (trừ khi có quyết định cơ quan có thẩm quyền).

Luồng kỹ thuật cơ bản: chủ sở hữu dữ liệu có ROLE_DATA_OWNER đăng ký niêm yết qua Data Listing Portal, khai báo mô tả, lược đồ, điều kiện, phạm vi, giá. Data Classification and Risk Engine phân loại dữ liệu, đánh giá nguy cơ tái định danh, kiểm tra dữ liệu có thuộc Quyết định số 20/2025/QĐ-TTg (từ chối nếu thuộc danh mục mà không có quyết định của cơ quan có thẩm quyền). Listing Hash Service tính listingHash; DataListingRegistry ghi giá trị băm qua registerListing(). Khi bên khai thác gửi yêu cầu cấp phép, License Management Service chuyển yêu cầu cho chủ sở hữu hoặc cơ quan có thẩm quyền phê duyệt tùy loại dữ liệu; sau khi phê duyệt, DataLicenseRegistry ghi giấy phép qua grantLicense(), LicenseSBT đúc Token định danh giấy phép gắn Hub ID bên khai thác. Khi bên khai thác truy vấn dữ liệu, Access Control Gateway kiểm chứng LicenseSBT, kiểm tra phạm vi, thời hạn, hạn mức; Re-identification Risk Control Service áp dụng các biện pháp kiểm soát (làm tròn, ẩn thuộc tính, giới hạn kết quả) đối với dữ liệu có nguy cơ tái định danh cao; DataAccessLog ghi mã tham chiếu phiên truy vấn. Re-identification Risk Control Service giám sát liên tục các mẫu truy vấn để phát hiện dấu hiệu kết hợp dữ liệu, vượt ngưỡng tần suất hoặc khối lượng; khi phát hiện bất thường, Access Control Gateway áp dụng biện pháp kiểm soát tăng cường (giảm hạn mức, tạm dừng truy cập) và License Management Service thông báo cho các bên liên quan; cơ quan giám sát có thể quyết định thu hồi giấy phép nếu vi phạm được xác nhận.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP5: M1: TC; M2: B; M3: B; M4: B; M5: B; M6: B; M7: B.

- **Mô đun 4 (bắt buộc):** LicenseSBT sử dụng TokenFactory của Mô đun 4 đúc token theo ERC-721 với transferable=false; ComplianceEngine chặn mọi lời gọi chuyển nhượng giấy phép, bảo đảm giấy phép khai thác không trở thành tài sản giao dịch.

- **Mô đun 2 (bắt buộc):** DataListingRegistry và DataAccessLog gọi ProofRegistry và BatchManager của Mô đun 2 để ghi bằng chứng niêm yết và nhật ký truy vấn.

- **Mô đun 3 (bắt buộc):** quản lý các vai trò ROLE_DATA_OWNER, ROLE_DATA_CONSUMER, ROLE_LISTING_ADMIN (cơ quan quản lý niêm yết), ROLE_DATA_AUDITOR (cơ quan giám sát).

- **Mô đun 5 (bắt buộc):** bốn hợp đồng thông minh riêng đăng ký vào ContractRegistry; nâng cấp theo Proxy Upgrade Pattern với đa ký và timelock 48 giờ.

- **Mô đun 6 (bắt buộc):** SP5 đăng ký vào ApplicationRegistry; AccessGate của Mô đun 6 kiểm soát truy cập ứng dụng.

- **Mô đun 7 (bắt buộc):** bên khai thác dữ liệu (cá nhân, doanh nghiệp, tổ chức) định danh bằng Hub ID; chủ sở hữu dữ liệu định danh bằng DID đăng ký tại IssuerWhitelist khi cần phát hành Chứng nhận xác minh.

Mức tùy chọn Mô đun 1 áp dụng khi có nhu cầu chia sẻ dữ liệu liên tỉnh hoặc liên quốc gia và được cơ quan có thẩm quyền phê duyệt.

5. Giao diện và tích hợp

SP5 tích hợp với bốn nhóm hệ thống nguồn: hệ thống dữ liệu mở của cơ quan nhà nước (các sở, ban, ngành có dữ liệu mở); hệ thống dữ liệu có giá trị gia tăng do doanh nghiệp tạo lập (niêm yết dữ liệu được cấp phép khai thác có phí); hệ thống quản lý dữ liệu của thành phố (đồng bộ danh mục dữ liệu); Cổng dữ liệu quốc gia và các hệ thống chia sẻ dữ liệu liên ngành (khi có quyết định cho phép).

Bảng C.6.2. Giao diện kỹ thuật chính của SP5

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Hệ thống dữ liệu của cơ quan nhà nước qua LGSP	REST trên HTTPS	mTLS + JWT + chữ ký số của cơ quan chủ sở hữu
Hệ thống dữ liệu của doanh nghiệp, tổ chức	REST + OAuth 2.0 Client Credentials Grant	mTLS + OAuth 2.0
Bên khai thác dữ liệu	Data Service and Marketplace Portal; API khai thác qua Access Control Gateway	JWT + Hub ID + LicenseSBT đính kèm
Cơ quan giám sát	Audit Trail Service; giao diện quản trị	mTLS + JWT + ROLE_DATA_AUDITOR
Chuỗi ngoài (chia sẻ dữ liệu liên tỉnh, liên quốc gia)	Qua Mô đun 1 khi được phê duyệt	Theo đặc tả Mô đun 1 tại Phần B Mục 1

Chuẩn kỹ thuật cốt lõi: DCAT (Data Catalog Vocabulary) của W3C và Dublin Core cho siêu dữ liệu; JSON, JSON-LD, CSV, Parquet cho định dạng trao đổi dữ liệu; REST + GraphQL cho API khai thác theo Nghị định số 278/2025/NĐ-CP; ERC-721 với transferable=false cho LicenseSBT; DID và Hub ID của Mô đun 7 cho định danh; Khung kiến trúc dữ liệu quốc gia tham chiếu Quyết định số 2439/QĐ-TTg. Các chuẩn mật mã chung (ECDSA secp256k1, SHA-256, keccak256, RFC 3161) áp dụng theo quy định tại Phần A Mục VII.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.6.3. Chỉ tiêu mức dịch vụ cốt lõi của SP5

Chỉ tiêu	Mức cam kết
Thời gian niêm yết mới từ khi chủ sở hữu xác nhận	≤ 10 phút với 95% niêm yết
Thời gian cấp giấy phép sau khi có phê duyệt	≤ 5 phút với 99% giấy phép
Thời gian kiểm tra quyền truy cập tại Access Control Gateway	≤ 500 mili-giây với 99% lượt
Thời gian phát hiện truy vấn bất thường từ khi vượt ngưỡng	≤ 5 phút
Tỷ lệ từ chối đúng dữ liệu thuộc Quyết định số 20/2025/QĐ-TTg (khi chưa có phép)	100%
Khả năng chịu tải Access Control Gateway	≥ 2.000 truy vấn/giây ở chế độ cao điểm

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút) áp dụng theo quy định chung tại Phần A Mục VII. Chỉ tiêu "từ chối đúng 100% dữ liệu thuộc danh mục dữ liệu quan trọng khi chưa có phép" là chỉ tiêu tuân thủ bắt buộc, kiểm chuẩn độc lập trước khi vận hành.

7. Điều kiện triển khai và giới hạn phạm vi

Điều kiện kỹ thuật triển khai SP5:

- Khung quản trị dữ liệu của thành phố đã được ban hành đầy đủ (phân loại dữ liệu, tiêu chí đánh giá nguy cơ tái định danh, biện pháp kiểm soát tăng cường, quy trình phê duyệt niêm yết và cấp phép);
- Danh mục dữ liệu mở của cơ quan nhà nước đã được chuẩn hoá và công bố;
- Hướng dẫn về phương pháp định giá dữ liệu và bảo vệ quyền sở hữu trí tuệ đối với dữ liệu giao dịch đã được ban hành;
- Chủ sở hữu dữ liệu tham gia đã đăng ký vào IssuerWhitelist của Mô đun 7 và IssuerRegistry của Mô đun 2 với phạm vi dữ liệu được niêm yết;
- Cơ chế kiểm tra dữ liệu thuộc Danh mục dữ liệu quan trọng, dữ liệu cốt lõi đã được tích hợp vào Data Classification and Risk Engine với danh mục cập nhật định kỳ theo Quyết định số 20/2025/QĐ-TTg;
- Bốn hợp đồng DataListingRegistry, DataLicenseRegistry, DataAccessLog, LicenseSBT đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;
- SP5 đã được đăng ký vào ApplicationRegistry của Mô đun 6 và chuyển sang trạng thái vận hành chính thức;

- Các sản phẩm Tầng 1 đã được đánh giá đủ cơ sở chuyển sang Tầng 3 theo lộ trình tại Bảng 3 Mục IV Chương III của Đề án.

Giới hạn phạm vi đặc tả của Phụ lục đối với SP5. Các nội dung sau thuộc hồ sơ thiết kế kỹ thuật dự án thành phần hoặc tài liệu vận hành, không thuộc phạm vi Phụ lục I:

- Danh mục cụ thể các bộ dữ liệu, dịch vụ dữ liệu đưa lên sàn trong giai đoạn đầu và lộ trình mở rộng;
- Tiêu chí chi tiết phân loại dữ liệu ba mức và tiêu chí đánh giá nguy cơ tái định danh ba mức;
- Phương pháp định giá dữ liệu, khung phí cấp phép khai thác;
- Tham số cấu hình chi tiết (hạn mức truy vấn theo loại dữ liệu, ngưỡng cảnh báo truy vấn bất thường, chu kỳ đánh giá rủi ro tự động);
- Thiết kế chi tiết giao diện Data Listing Portal và Data Service and Marketplace Portal;
- Quy trình phê duyệt niêm yết và cấp phép cho từng loại dữ liệu (dữ liệu mở, dữ liệu được cấp phép, dữ liệu nhạy cảm);
- Cơ chế giải quyết tranh chấp giữa chủ sở hữu và bên khai thác về phạm vi và chất lượng dữ liệu.

SP6 - Sàn giao dịch tài sản sở hữu trí tuệ tích hợp blockchain

1. Định vị sản phẩm

SP6 thuộc Tầng 3 của Đề án, triển khai trong giai đoạn 2028 - 2030. Sản phẩm là nền tảng ghi nhận bằng chứng sáng tạo, đồng bộ trạng thái văn bằng bảo hộ, phát hành Token đại diện tài sản sở hữu trí tuệ và ghi nhận giao dịch cấp phép, chuyển nhượng có kiểm soát đối với tài sản trí tuệ.

Nguyên tắc xuyên suốt SP6 là "blockchain chỉ là lớp tin cậy số bổ sung, không thay thế thẩm quyền xác lập quyền, đăng ký quyền và quản lý nhà nước về sở hữu trí tuệ theo Luật Sở hữu trí tuệ". Bằng chứng sáng tạo ghi lên DNC-Chain không thay thế đơn đăng ký bảo hộ; Token IP chỉ được đúc sau khi cơ quan nhà nước có thẩm quyền đã cấp văn bằng bảo hộ hoặc giấy chứng nhận quyền tác giả; giao dịch chuyển nhượng trên chuỗi có giá trị bằng chứng bổ sung, thủ tục đăng ký chuyển nhượng tại cơ quan nhà nước vẫn thực hiện theo quy định pháp luật.

Theo quyết định chốt về thuật ngữ, SP6 sử dụng thống nhất cụm từ "Token đại diện tài sản sở hữu trí tuệ theo chuẩn ERC-721 có thể chuyển nhượng có kiểm soát qua Compliance Layer", rút gọn thành "Token IP"; không sử dụng thuật ngữ "NFT" đơn thuần để tránh hiểu nhầm sang thị trường NFT thương mại và bảo đảm thống nhất với Bảng 4.2 Phần B (nhóm Token đại diện tài sản có thể chuyển nhượng có kiểm soát).

SP6 là sản phẩm duy nhất trong 10 sản phẩm có Mô đun 1 ở mức bắt buộc (liên thông bằng chứng IP với chuỗi ngoài khi quốc tế hoá) và Mô đun 4 ở mức bắt buộc cốt lõi (Token IP có thể chuyển nhượng có kiểm soát).

2. Chức năng nghiệp vụ chính

SP6 cung cấp sáu nhóm chức năng:

- Ghi bằng chứng sáng tạo với dấu thời gian bất biến trước khi nộp đơn đăng ký bảo hộ (tham chiếu thời điểm sáng tạo);
- Đồng bộ trạng thái văn bằng bảo hộ từ cơ sở dữ liệu của Cục Sở hữu trí tuệ và giấy chứng nhận quyền tác giả từ Cục Bản quyền tác giả;
- Đúc Token IP theo ERC-721 sau khi văn bằng được cấp và đồng bộ;
- Quản lý vòng đời cấp phép khai thác IP (cấp mới, gia hạn, điều chỉnh, chấm dứt) với ký số đa bên;
- Chuyển nhượng Token IP có kiểm soát qua Compliance Layer;
- Tra cứu trạng thái IP phục vụ ngân hàng, tổ chức tín dụng (thẩm định tài sản bảo đảm) và tòa án (giải quyết tranh chấp).

3. Kiến trúc kỹ thuật đặc thù

SP6 tổ chức theo kiến trúc hai lớp: lớp off-chain đặt tại hạ tầng dữ liệu của thành phố và cổng tích hợp với cơ quan nhà nước về sở hữu trí tuệ; lớp on-chain gồm bốn hợp đồng thông minh riêng trên DNC-Chain.

Bảng C.7.1. Cấu phần off-chain và on-chain của SP6

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Creation Proof Gateway	Tiếp nhận yêu cầu ghi bằng chứng sáng tạo; chỉ tiếp nhận giá trị băm của tài liệu sáng tạo, không nhận nội dung chi tiết
Off-chain	IP Registry Sync Service	Đồng bộ trạng thái văn bằng bảo hộ từ Cục Sở hữu trí tuệ (sáng chế, giải pháp hữu ích, kiểu dáng, nhãn hiệu); đồng bộ giấy chứng nhận từ Cục Bản quyền tác giả
Off-chain	KYC Service	Xác minh danh tính cá nhân và tư cách pháp nhân trước khi ghi bằng chứng hoặc đúc Token IP; sử dụng Hub ID của Mô đun 7
Off-chain	License Management Service	Tiếp nhận yêu cầu cấp phép khai thác IP; ký số giữa các bên; điều phối vòng đời cấp phép
Off-chain	IP Marketplace Portal	Cổng kết nối cung cầu khai thác IP; tìm kiếm theo lĩnh vực, tình trạng bảo hộ, loại quyền

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Financial Verification API	Giao diện cho ngân hàng, tổ chức tín dụng, tòa án tra cứu trạng thái IP phục vụ thẩm định tài sản bảo đảm và giải quyết tranh chấp
Off-chain	Transfer Notary Service	Ghi nhận giao dịch chuyển nhượng on-chain làm bằng chứng bổ sung; nhắc thực hiện thủ tục đăng ký tại cơ quan nhà nước
On-chain	CreationProofRegistry	Hợp đồng thông minh riêng; ghi bằng chứng sáng tạo với dấu thời gian RFC 3161; kế thừa ProofRegistryTemplate của Mô đun 5
On-chain	IPTokenRegistry	Hợp đồng thông minh riêng; đúc và quản lý Token IP theo ERC-721 có kiểm soát qua Compliance Layer của Mô đun 4
On-chain	IPLicenseRegistry	Hợp đồng thông minh riêng; quản lý vòng đời cấp phép khai thác IP với ký số đa bên; sử dụng EscrowTemplate của Mô đun 5 khi có yếu tố ký quỹ
On-chain	IPTransferLog	Hợp đồng thông minh riêng; ghi nhận sự kiện chuyển nhượng Token IP làm bằng chứng bổ sung

Bốn hợp đồng thông minh riêng tuân thủ ERC-721, EIP-712, ERC-165, RFC 3161. Lưu ý kỹ thuật quan trọng: IPTokenRegistry không tự tạo chuẩn ERC-721 mới; mọi thao tác đúc và chuyển nhượng Token IP đều thực hiện qua TokenFactory và ComplianceEngine của Mô đun 4, bảo đảm thống nhất với thiết kế Phần B và tận dụng khả năng kiểm soát tuân thủ tập trung đã được kiểm toán. Cấu trúc dữ liệu bằng chứng sáng tạo trên CreationProofRegistry gồm các trường kỹ thuật (proofId, creationHash SHA-256, authorHubId, creationTypeCode, timestamp RFC 3161, metadataURI chỉ chứa tên và mô tả ngắn, statusCode); Token IP trên IPTokenRegistry lưu tokenId, creationProofId (tham chiếu bằng chứng sáng tạo gốc), officialRegistrationRefHash (số văn bằng bảo hộ đã bấm), ipTypeCode, ownerHubId, scopeHash, issuedAt, expiresAt theo thời hạn pháp luật, statusCode. Danh sách trường loại trừ không được ghi lên chuỗi gồm: toàn văn tác phẩm, toàn văn sáng chế, toàn văn bản mô tả kỹ thuật, toàn văn kiểu dáng công nghiệp, tệp nguồn phần mềm; bí mật kinh doanh, know-how, công thức kỹ thuật chưa công bố; nội dung chi tiết hợp đồng cấp phép và chuyển nhượng; giá trị giao dịch cụ thể và phương thức thanh toán; thông tin cá nhân chi tiết của tác giả, nhà phát minh; thông tin tài chính của các bên; báo cáo đánh giá, thẩm định IP.

Luồng kỹ thuật cơ bản: đối với bằng chứng sáng tạo, tác giả tính SHA-256 của tài liệu sáng tạo tại thiết bị của mình, chỉ gửi giá trị băm (không gửi nội dung) qua Creation

Proof Gateway; KYC Service xác minh danh tính; CreationProofRegistry ghi qua ProofRegistry của Mô đun 2 với dấu thời gian RFC 3161; tác giả nhận biên lai kèm proofId phục vụ đối chiếu khi nộp đơn đăng ký bảo hộ. Đối với đúc Token IP, IP Registry Sync Service đồng bộ trạng thái văn bằng từ cơ quan nhà nước về IP; IPTokenRegistry kiểm tra bằng chứng sáng tạo gốc (nếu có) và gọi TokenFactory của Mô đun 4 đúc Token IP; ComplianceEngine của Mô đun 4 ghi quy tắc tuân thủ (phạm vi chuyển nhượng, allowlist chủ thể, trạng thái văn bằng); Mô đun 7 phát hành Chứng nhận xác minh quyền tác giả hoặc quyền sở hữu. Khi chuyển nhượng Token IP, ComplianceEngine kiểm tra bốn điều kiện trước mỗi giao dịch: trạng thái hiệu lực của văn bằng, bên nhận thuộc allowlist, không có giấy phép độc quyền đang hiệu lực hạn chế chuyển nhượng, mục đích chuyển nhượng phù hợp; IPTokenRegistry thực hiện chuyển nhượng qua TransferManager của Mô đun 4; IPTransferLog ghi giao dịch làm bằng chứng bổ sung; Transfer Notary Service nhắc các bên thực hiện thủ tục đăng ký chuyển nhượng tại cơ quan nhà nước có thẩm quyền.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP6: **M1: B**; M2: B; M3: B; **M4: BB**; M5: B; M6: B; M7: B. SP6 là sản phẩm duy nhất có Mô đun 4 ở mức bắt buộc cốt lõi và Mô đun 1 ở mức bắt buộc.

- **Mô đun 4 (bắt buộc cốt lõi):** IPTokenRegistry sử dụng TokenFactory của Mô đun 4 đúc Token IP theo ERC-721; ComplianceEngine thực thi quy tắc tuân thủ trước mỗi lần chuyển nhượng (kiểm tra bốn điều kiện đã nêu); TokenLedger lưu lịch sử số dư và giao dịch Token IP. Không có Mô đun 4, sản phẩm không vận hành được.

- **Mô đun 1 (bắt buộc):** cho phép chia sẻ bằng chứng IP với chuỗi ngoài khi có nhu cầu liên thông quốc tế (WIPO, blockchain cấp phép của các cơ quan IP nước ngoài) và được cơ quan có thẩm quyền phê duyệt. Đây là điểm khác biệt quan trọng của SP6 so với *10 sản phẩm* còn lại.

- **Mô đun 2 (bắt buộc):** CreationProofRegistry gọi ProofRegistry của Mô đun 2 ghi bằng chứng sáng tạo.

- **Mô đun 3 (bắt buộc):** quản lý các vai trò ROLE_IP_OWNER (chủ sở hữu IP), ROLE_IP_LICENSEE (bên nhận cấp phép), ROLE_IP_ADMIN (cơ quan quản lý sản), ROLE_IP_REGISTRY_SYNC (công đồng bộ với cơ quan nhà nước về IP), ROLE_FIN_VERIFIER (ngân hàng, tổ chức tín dụng), ROLE_IP_AUDITOR (cơ quan thanh tra, tòa án).

- **Mô đun 5 (bắt buộc):** bốn hợp đồng thông minh riêng đăng ký vào ContractRegistry; IPTokenRegistry kế thừa TokenStandardTemplate; IPLicenseRegistry sử dụng EscrowTemplate khi có yêu tố ký quỹ.

- **Mô đun 6 (bắt buộc):** SP6 đăng ký vào ApplicationRegistry; AccessGate của Mô đun 6 kiểm soát truy cập cấp ứng dụng đối với Financial Verification API.

- **Mô đun 7 (bắt buộc):** chủ sở hữu IP và bên nhận cấp phép được định danh bằng Hub ID; tác giả cá nhân được cấp VC về quyền tác giả.

5. Giao diện và tích hợp

SP6 tích hợp với năm nhóm hệ thống nguồn: cơ sở dữ liệu sáng chế, giải pháp hữu ích, kiểu dáng công nghiệp, nhãn hiệu tại Cục Sở hữu trí tuệ (Bộ Khoa học và Công nghệ); cơ sở dữ liệu quyền tác giả, quyền liên quan tại Cục Bản quyền tác giả (Bộ Văn hoá, Thể thao và Du lịch); hệ thống nghiệp vụ của ngân hàng và tổ chức tín dụng (tra cứu trạng thái IP phục vụ thẩm định tài sản bảo đảm); hệ thống nghiệp vụ của tòa án (tra cứu lịch sử giao dịch IP phục vụ giải quyết tranh chấp); hệ thống quản lý hoạt động khoa học, công nghệ và đổi mới sáng tạo của thành phố. **Việc tích hợp với Cục Sở hữu trí tuệ và Cục Bản quyền tác giả phải có thỏa thuận ủy quyền chính thức với các cơ quan nhà nước về IP và chỉ đề đồng bộ trạng thái; không cho phép SP6 tự xác lập quyền.**

Bảng C.7.2. Giao diện kỹ thuật chính của SP6

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Cục Sở hữu trí tuệ, Cục Bản quyền tác giả	IP Registry Sync Service theo thỏa thuận ủy quyền	mTLS + OAuth 2.0 Client Credentials Grant; có thể có webhook
Chủ sở hữu IP, tác giả, bên nhận cấp phép	IP Marketplace Portal; Creation Proof Gateway	JWT + Hub ID + chữ ký số ERC-191
Ngân hàng, tổ chức tín dụng	Financial Verification API	mTLS + JWT + ROLE_FIN_VERIFIER
Tòa án có thẩm quyền	Financial Verification API (mở rộng)	mTLS + JWT + ROLE_IP_AUDITOR
Chuỗi ngoài khi liên thông quốc tế (WIPO, chuỗi IP nước ngoài được phê duyệt)	Qua Mô đun 1 - Cầu nối đa chuỗi	Theo đặc tả Mô đun 1 tại Phần B Mục 1

Chuẩn kỹ thuật cốt lõi: ERC-721 có kiểm soát qua ComplianceEngine của Mô đun 4 cho Token IP; tiêu chuẩn của WIPO cho dữ liệu sáng chế, nhãn hiệu, kiểu dáng công nghiệp khi liên thông quốc tế; W3C Verifiable Credentials Data Model **v2.0** cho Chứng nhận xác minh quyền tác giả; DID và Hub ID của Mô đun 7 cho định danh. Các chuẩn mật mã chung (ECDSA secp256k1, SHA-256, keccak256, RFC 3161) áp dụng theo quy định tại Phần A Mục VII.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.7.3. Chỉ tiêu mức dịch vụ cốt lõi của SP6

Chỉ tiêu	Mức cam kết
Thời gian ghi bằng chứng sáng tạo từ khi chủ thể gửi giá trị băm	≤ 30 giây với 99% bằng chứng tính theo tháng
Thời gian đồng bộ trạng thái văn bằng từ cơ quan nhà nước (nếu có webhook)	≤ 10 phút kể từ thời điểm cơ quan nhà nước ban hành
Thời gian đúc Token IP sau khi xác nhận điều kiện	≤ 60 giây với 99% Token tính theo tháng
Thời gian tra cứu qua Financial Verification API	≤ 3 giây với 99% lượt
Tỷ lệ từ chối đúng yêu cầu đúc Token IP khi chưa có văn bằng hoặc giấy chứng nhận	100%
Tỷ lệ thực thi đúng quy tắc Compliance Layer trước chuyển nhượng (bốn điều kiện)	100%

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút) áp dụng theo quy định chung tại Phần A Mục VII. Hai chỉ tiêu "từ chối đúng 100% yêu cầu đúc khi chưa có văn bằng" và "thực thi đúng 100% quy tắc Compliance Layer" là chỉ tiêu tuân thủ bắt buộc, kiểm chuẩn độc lập trước khi vận hành do bản chất pháp lý của sản phẩm.

7. Điều kiện triển khai và giới hạn phạm vi

Điều kiện kỹ thuật triển khai SP6:

- Thỏa thuận ủy quyền đồng bộ dữ liệu giữa SP6 và Cục Sở hữu trí tuệ, Cục Bản quyền tác giả đã được ký kết; API đồng bộ đã sẵn sàng, có tài khoản kỹ thuật được cấp;
- Quy chế hoạt động của sàn đã được ban hành, xác định rõ: bằng chứng trên chuỗi không thay thế thẩm quyền xác lập quyền; giao dịch chuyển nhượng trên chuỗi có giá trị bổ sung, không thay thế thủ tục đăng ký tại cơ quan nhà nước;
- Chủ thể tham gia sàn đã KYC thành công qua KYC Service và có Hub ID hợp lệ;
- Khóa ký số các bên đã đăng ký vào KeyRegistry của Mô đun 3;
- Allowlist chủ thể được phép nhận chuyển nhượng Token IP đã được xác lập;
- Bốn hợp đồng CreationProofRegistry, IPTokenRegistry, IPLicenseRegistry, IPTransferLog đã hoàn thành kiểm toán bảo mật độc lập theo Phần A Mục XII;
- Quy tắc Compliance Layer của Mô đun 4 cho Token IP đã được cấu hình (bốn điều kiện kiểm tra trước chuyển nhượng) và đã được kiểm thử;

- Mô đun 1 đã vận hành ổn định với danh sách chuỗi ngoài được phép liên thông quốc tế đã phê duyệt;

- SP6 đã được đăng ký vào ApplicationRegistry của Mô đun 6 và chuyển trạng thái vận hành chính thức;

- Các sản phẩm Tầng 1 đã được đánh giá đủ cơ sở chuyển sang Tầng 3 theo lộ trình tại Bảng 3 Mục IV Chương III của Đề án.

Giới hạn phạm vi đặc tả của Phụ lục đối với SP6. Các nội dung sau thuộc hồ sơ thiết kế kỹ thuật dự án thành phần hoặc tài liệu vận hành, không thuộc phạm vi Phụ lục I:

- Thỏa thuận ủy quyền đồng bộ dữ liệu chi tiết với Cục Sở hữu trí tuệ và Cục Bản quyền tác giả (phạm vi, trách nhiệm, cơ chế giải quyết tranh chấp);

- Lược đồ chi tiết dữ liệu đồng bộ từ cơ quan nhà nước về IP theo từng loại quyền (sáng chế, nhãn hiệu, kiểu dáng công nghiệp, quyền tác giả);

- Allowlist cụ thể các chủ thể được phép nhận chuyển nhượng Token IP;

- Tham số cấu hình chi tiết của Compliance Layer cho từng loại IP;

- Thiết kế chi tiết IP Marketplace Portal;

- Quy trình phối hợp với tòa án khi có tranh chấp IP;

- Quy trình xử lý trường hợp văn bằng bị hủy sau khi Token IP đã được đúc và có giao dịch chuyển nhượng;

- Danh sách chuỗi ngoài được phép liên thông quốc tế và quy trình phê duyệt bổ sung.

SP7 - Chương trình khách hàng trung thành của thành phố (City Loyalty Program) tích hợp blockchain

1. Định vị sản phẩm

SP7 thuộc Tầng 3 của Đề án, triển khai trong giai đoạn 2028 - 2030. Sản phẩm là nền tảng điểm thưởng số dùng chung trên phạm vi thành phố, kết nối các doanh nghiệp cung cấp dịch vụ du lịch, dịch vụ đô thị qua cơ chế tích hợp đơn giản.

Nguyên tắc xuyên suốt SP7 là "DaNang Point là điểm thưởng dịch vụ, không phải tài sản tài chính; không giao dịch trên sàn; không quy đổi sang tiền pháp định"; cơ chế vận hành tương tự các chương trình miles của hàng không và điểm thưởng thẻ ngân hàng. Token DaNang Point được triển khai theo chuẩn ERC-20 tùy chỉnh với Compliance Layer chặn chuyển nhượng ngoài hệ sinh thái và chặn quy đổi sang tiền pháp định, thống nhất với Bảng 4.2 Phần B (nhóm Token điểm thưởng). SP7 có Mô đun 4 ở mức bắt buộc cốt lõi do bản chất sản phẩm là quản lý token điểm thưởng; SP7 không sử dụng Mô đun 1 (không liên thông liên chuỗi).

2. Chức năng nghiệp vụ chính

SP7 cung cấp năm nhóm chức năng:

- Đăng ký tham gia chương trình của người dùng qua xác minh VNeID và cấp Hub ID;
- Tích điểm khi người dùng sử dụng dịch vụ của doanh nghiệp đối tác, có đối chiếu chống giả mạo;
- Đổi thưởng trong hệ sinh thái đối tác đổi thưởng, chặn tuyệt đối việc quy đổi sang tiền pháp định;
- Phân tích hành vi du lịch ở dạng tổng hợp, ẩn danh phục vụ quản lý thành phố và hoạch định chính sách;
- Xử lý yêu cầu rút, khiếu nại, hoàn trả điểm theo pháp luật về bảo vệ quyền lợi người tiêu dùng.

3. Kiến trúc kỹ thuật đặc thù

SP7 tổ chức theo kiến trúc hai lớp: lớp off-chain đặt tại hạ tầng dữ liệu của thành phố và hệ thống doanh nghiệp đối tác; lớp on-chain gồm ba hợp đồng thông minh riêng trên DNC-Chain.

Bảng C.8.1. Cấu phần off-chain và on-chain của SP7

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Merchant Integration Gateway	Tiếp nhận sự kiện giao dịch dịch vụ từ doanh nghiệp đối tác; xác minh doanh nghiệp; kiểm tra lược đồ giao dịch
Off-chain	Anti-Fraud Service	Phát hiện giao dịch tích điểm giả mạo qua đối chiếu với hệ thống nguồn của doanh nghiệp
Off-chain	Point Calculation Engine	Tính số điểm tích lũy theo tỷ lệ đã đăng ký của từng doanh nghiệp và loại dịch vụ
Off-chain	Mobile Wallet Backend	Hỗ trợ ứng dụng ví: theo dõi điểm, đổi thưởng, lịch sử giao dịch
Off-chain	Redemption Service	Xử lý yêu cầu đổi thưởng; kiểm tra hạn mức, ưu đãi, đối tác đổi thưởng
Off-chain	Merchant SDK	Thư viện tích hợp cho doanh nghiệp đối tác gửi sự kiện giao dịch
Off-chain	Anonymized Analytics Engine	Phân tích hành vi du lịch ở dạng tổng hợp, ẩn danh; không truy cập dữ liệu cá nhân chi tiết

Lớp	Cấu phần	Chức năng kỹ thuật chính
Off-chain	Consumer Protection Mô đun	Xử lý khiếu nại, hoàn trả điểm theo pháp luật về bảo vệ quyền lợi người tiêu dùng
On-chain	PointToken	Hợp đồng thông minh riêng; triển khai Token DaNang Point theo ERC-20 tùy chỉnh với Compliance Layer chặn chuyển nhượng ngoài hệ sinh thái và chặn quy đổi sang tiền pháp định
On-chain	PointTransactionLog	Hợp đồng thông minh riêng; ghi lịch sử tích điểm, đổi thưởng
On-chain	MerchantRegistry	Hợp đồng thông minh riêng; danh mục doanh nghiệp đối tác được ủy quyền phát sinh giao dịch điểm

Ba hợp đồng thông minh riêng tuân thủ ERC-20, ERC-165, EIP-712. Cấu trúc dữ liệu giao dịch trên PointTransactionLog gồm các trường kỹ thuật (transactionId, userHubId, merchantDID, transactionTypeCode - tích điểm/đổi thưởng/điều chỉnh/hoàn trả, pointAmount, merchantTxRefHash - mã giao dịch gốc tại doanh nghiệp đã bấm, timestamp, statusCode); MerchantRegistry lưu merchantId, merchantDID, merchantTypeCode theo loại dịch vụ (lưu trú, ẩm thực, tham quan, mua sắm, vận chuyển, dịch vụ công), earnRate, isRedemptionPartner. Danh sách trường loại trừ không được ghi lên chuỗi gồm: họ tên, số định danh cá nhân, ngày sinh, địa chỉ, số điện thoại, địa chỉ thư điện tử của người dùng; nội dung chi tiết đơn hàng (tên món, tên khách sạn, phòng cụ thể, dịch vụ chi tiết); số tiền thanh toán thực tế, phương thức thanh toán, số thẻ ngân hàng; hình ảnh, video về chuyến đi, sở thích du lịch cá nhân chi tiết; lịch trình di chuyển chi tiết (tọa độ GPS, thời điểm đến từng địa điểm); thông tin bạn đồng hành; bí mật kinh doanh của doanh nghiệp đối tác (giá thực tế, biên lợi nhuận, danh sách khách hàng).

Luồng kỹ thuật cơ bản: người dùng đăng ký qua ứng dụng ví DaNang Point, xác minh qua VNeID theo luồng Identity Gateway của Mô đun 3 và được cấp Hub ID qua Mô đun 7. Khi người dùng sử dụng dịch vụ tại đối tác (quét mã QR định danh DaNang Point hoặc cho đối tác quét Hub ID trên ứng dụng ví), hệ thống doanh nghiệp phát sinh giao dịch dịch vụ; Merchant SDK gửi sự kiện tích điểm kèm mã giao dịch gốc (đã bấm) qua Merchant Integration Gateway. Anti-Fraud Service đối chiếu với hệ thống nguồn của doanh nghiệp để phát hiện giao dịch giả mạo; Point Calculation Engine tính số điểm theo tỷ lệ đã đăng ký; PointToken gọi mint() qua TokenFactory của Mô đun 4; ComplianceEngine xác nhận doanh nghiệp thuộc allowlist; PointTransactionLog ghi giao dịch. Khi người dùng đổi thưởng, Redemption Service kiểm tra số dư, hạn mức, trạng thái đối tác đổi thưởng; ComplianceEngine của Mô đun 4 xác nhận đối tác đổi thưởng thuộc allowlist (có ROLE_REDEMPTION_PARTNER) và chặn tuyệt đối mọi nỗ lực quy đổi sang tiền pháp định; PointToken gọi burn() số điểm tương ứng; người dùng nhận mã đổi thưởng (voucher, QR) để sử dụng tại đối tác đổi thưởng. Đối với phân tích hành vi du lịch phục vụ quản lý thành phố, Anonymized Analytics Engine tổng hợp dữ liệu giao dịch điểm ở cấp nhóm (theo loại doanh nghiệp, khu vực, khoảng thời gian) với

ngưỡng tổng hợp tối thiểu (100 người dùng hoặc 500 giao dịch mỗi nhóm) để tránh tái định danh; báo cáo tổng hợp không chứa thông tin cá nhân.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP7: **M1: -**; M2: TC; M3: B; **M4: BB**; M5: B; M6: B; M7: B.

- **Mô đun 4 (bắt buộc cốt lõi):** PointToken sử dụng TokenFactory của Mô đun 4 tạo Token DaNang Point theo ERC-20 tùy chỉnh; ComplianceEngine thực thi quy tắc **chặn tuyệt đối** mọi lời gọi chuyển nhượng ra ngoài hệ sinh thái đối tác đã đăng ký và **chặn tuyệt đối** mọi nỗ lực quy đổi sang tiền pháp định; TokenLedger lưu lịch sử số dư và giao dịch. Hai ràng buộc này là ràng buộc kỹ thuật cứng được cài đặt ở cấp mã nguồn hợp đồng, không thể vượt qua mà không nâng cấp hợp đồng qua quy trình của Mô đun 5 với sự phê duyệt của Ủy ban nhân dân thành phố.

- **Mô đun 3 (bắt buộc):** quản lý các vai trò ROLE_MERCHANT (doanh nghiệp đối tác phát sinh giao dịch), ROLE_REDEMPTION_PARTNER (doanh nghiệp đối tác đổi thưởng), ROLE_LOYALTY_ADMIN (cơ quan quản lý chương trình), ROLE_LOYALTY_AUDITOR (cơ quan giám sát).

- **Mô đun 5 (bắt buộc):** ba hợp đồng thông minh riêng đăng ký vào ContractRegistry; PointToken kế thừa TokenStandardTemplate; nâng cấp theo Proxy Upgrade Pattern với đa ký và timelock 48 giờ.

- **Mô đun 6 (bắt buộc):** SP7 đăng ký vào ApplicationRegistry; AccessGate của Mô đun 6 kiểm soát truy cập ứng dụng.

- **Mô đun 7 (bắt buộc):** người dùng tham gia chương trình được xác minh qua VNeID và cấp Hub ID qua Mô đun 7; số dư điểm gắn với Hub ID của người dùng, không lưu họ tên, số định danh cá nhân trên chuỗi.

Mức tùy chọn Mô đun 2 áp dụng khi thông lượng cao (PointTransactionLog sử dụng BatchManager gom lô).

- **Mô đun 1 không sử dụng.** SP7 là chương trình nội bộ thành phố, không kết nối liên chuỗi.

5. Giao diện và tích hợp

SP7 tích hợp với sáu nhóm hệ thống nguồn của doanh nghiệp đối tác qua Merchant SDK: hệ thống bán hàng tại cơ sở lưu trú (khách sạn, khu nghỉ dưỡng); hệ thống bán hàng tại cơ sở ẩm thực (nhà hàng, quán cà phê); hệ thống bán vé điểm tham quan (khu vui chơi); hệ thống bán hàng tại trung tâm mua sắm (cửa hàng, siêu thị); hệ thống dịch vụ vận chuyển (taxi, xe buýt du lịch); hệ thống của cơ quan quản lý có dịch vụ công có thu phí phù hợp khung pháp luật. SP7 không tích hợp qua LGSP do là chương trình của doanh nghiệp đối tác và thành phố cùng phối hợp; tuy nhiên các cơ quan quản lý của thành phố có thể đăng ký tham gia theo vai trò merchant đối với dịch vụ công có thu phí.

Bảng C.8.2. Giao diện kỹ thuật chính của SP7

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
--------------------	-----------	----------------

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Hệ thống của doanh nghiệp đối tác	Merchant SDK; REST trên HTTPS với mTLS	mTLS + JWT + chữ ký số ERC-191 của doanh nghiệp
Người dùng	Ứng dụng ví DaNang Point; luồng xác minh qua VNeID	OpenID Connect qua VNeID; khoá riêng người dùng
Cơ quan quản lý chương trình	Giao diện quản trị; Consumer Protection Mô đun	JWT + ROLE_LOYALTY_ADMIN
Cơ quan giám sát	Anonymized Analytics Engine; giao diện báo cáo	mTLS + JWT + ROLE_LOYALTY_AUDITOR

Chuẩn kỹ thuật cốt lõi: ERC-20 tùy chỉnh với Compliance Layer cho Token DaNang Point; DID cho doanh nghiệp đối tác và Hub ID cho người dùng (cấp qua VNeID và Mô đun 7); OpenID Connect qua VNeID theo Luồng Identity Gateway của Mô đun 3. Các chuẩn mật mã chung (ECDSA secp256k1, SHA-256, keccak256, RFC 3161) áp dụng theo quy định tại Phần A Mục VII.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.8.3. Chỉ tiêu mức dịch vụ cốt lõi của SP7

Chỉ tiêu	Mức cam kết
Thời gian ghi giao dịch tích điểm từ khi merchant gửi sự kiện	≤ 10 giây với 99% giao dịch tính theo tháng
Thời gian xử lý đổi thưởng từ khi người dùng xác nhận	≤ 5 giây với 99% giao dịch tính theo tháng
Thời gian hiển thị số dư điểm cập nhật trên ứng dụng ví	≤ 3 giây sau khi ghi giao dịch
Tỷ lệ thực thi đúng Compliance Layer (chặn chuyển nhượng ngoài hệ sinh thái)	100%

Chỉ tiêu	Mức cam kết
Tỷ lệ thực thi đúng Compliance Layer (chặn quy đổi sang tiền pháp định)	100%
Khả năng chịu tải ứng dụng ví giờ cao điểm	≥ 500 yêu cầu/giây

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút) áp dụng theo quy định chung tại Phần A Mục VII. Hai chỉ tiêu **"thực thi đúng 100% Compliance Layer"** là chỉ tiêu tuân thủ then chốt của SP7, kiểm chuẩn độc lập trước khi vận hành và định kỳ trong quá trình vận hành; bất kỳ sai sót nào của Compliance Layer (cho phép chuyển nhượng ngoài hệ sinh thái hoặc quy đổi sang tiền pháp định) đều phải được xử lý khẩn cấp theo quy trình tại Phần B Mục 4.

7. Điều kiện triển khai và giới hạn phạm vi

Điều kiện kỹ thuật triển khai SP7:

- Quy chế hoạt động chương trình DaNang Point đã được ban hành, xác định rõ nguyên tắc "không phải tài sản tài chính, không giao dịch trên sàn, không quy đổi sang tiền pháp định";
- Khung pháp lý về bảo vệ quyền lợi người tiêu dùng đã được rà soát; quy trình xử lý khiếu nại và hoàn trả điểm đã được ban hành;
- Doanh nghiệp đối tác đã ký thỏa thuận tham gia chương trình và được đăng ký vào MerchantRegistry với phạm vi, tỷ lệ tích điểm, vai trò (phát sinh hoặc đổi thưởng);
- Khóa ký số doanh nghiệp đối tác đã đăng ký vào KeyRegistry của Mô đun 3;
- Anti-Fraud Service đã được kiểm thử với dữ liệu thử nghiệm từ các doanh nghiệp đối tác;
- Quy tắc Compliance Layer cho Token DaNang Point đã được cấu hình (chặn chuyển nhượng ngoài hệ sinh thái, chặn quy đổi sang tiền pháp định) và đã được kiểm thử chuyên sâu;
- Ba hợp đồng PointToken, PointTransactionLog, MerchantRegistry đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;
- SP7 đã được đăng ký vào ApplicationRegistry của Mô đun 6 và chuyển sang trạng thái vận hành chính thức;
- Các sản phẩm Tầng 1 đã được đánh giá đủ cơ sở chuyển sang Tầng 3 theo lộ trình tại Bảng 3 Mục IV Chương III của Đề án.

Giới hạn phạm vi đặc tả của Phụ lục đối với SP7. Các nội dung sau thuộc hồ sơ thiết kế kỹ thuật dự án thành phần hoặc tài liệu vận hành, không thuộc phạm vi Phụ lục I:

- Danh sách cụ thể các doanh nghiệp đối tác tham gia chương trình trong giai đoạn đầu và lộ trình mở rộng;
- Chính sách tỷ lệ tích điểm chi tiết theo từng loại dịch vụ và từng doanh nghiệp đối tác;
- Hạn mức tích điểm tối đa mỗi người dùng mỗi ngày;
- Danh mục ưu đãi đổi thưởng và giá trị đổi thưởng chi tiết;
- Thời hạn hiệu lực của điểm và cơ chế tự động hết hạn;
- Thiết kế chi tiết ứng dụng ví DaNang Point;
- Quy trình Anti-Fraud Service chi tiết và ngưỡng cảnh báo cho từng loại bất thường;
- Quy trình xử lý khiếu nại và hoàn trả điểm theo pháp luật về bảo vệ quyền lợi người tiêu dùng;
- Cơ chế phối hợp giữa cơ quan quản lý chương trình và các sở, ngành tham gia theo vai trò merchant cho dịch vụ công.

SP8 - Nền tảng chuyển đổi tài sản mã hóa sang tiền pháp định

1. Định vị sản phẩm

SP8 thuộc Tầng 4 của Đề án, triển khai theo cơ chế sandbox của thành phố Đà Nẵng trên cơ sở Nghị quyết số 55/2024/NQ-HĐND ngày 13/12/2024 của Hội đồng nhân dân thành phố và Quyết định số 1181/QĐ-UBND ngày 26/8/2025 của Ủy ban nhân dân thành phố. SP8 không phải ứng dụng công dùng chung của thành phố, không cấp sandbox mới và không thay thế cơ chế hiện hành; Đề án thực hiện vai trò ghi nhận, tiếp nhận, định vị và điều phối ở cấp thành phố.

Bản chất SP8 là nền tảng nghiệp vụ do doanh nghiệp tham gia thử nghiệm xây dựng và vận hành end-to-end (đăng ký tài khoản, xác minh định danh điện tử, nạp và rút tài sản mã hoá, chuyển đổi sang tiền Việt Nam đồng). DNC-Chain không tiếp nhận chi tiết giao dịch cá nhân, không lưu số dư tài khoản, không lưu dữ liệu người dùng cuối. Phụ lục I chỉ đặc tả 03 cấu phần giao tiếp với DNC-Chain thuộc phần công vụ phục vụ chức năng quản lý nhà nước, giám sát, đối soát, truy vết, hậu kiểm; phần thương mại của nền tảng nghiệp vụ do doanh nghiệp đầu tư, không thuộc phạm vi Phụ lục.

SP8 không triển khai hợp đồng thông minh riêng trên DNC-Chain; chỉ sử dụng ConversionGateway của Mô đun 4 làm điểm tiếp xúc.

2. Chức năng nghiệp vụ chính

Phạm vi chức năng thuộc Phụ lục I (chỉ 03 cấu phần giao tiếp với DNC-Chain):

- Ghi bằng chứng báo cáo tuân thủ định kỳ (KYC tổng hợp, AML/CFT, giao dịch theo ngưỡng) lên DNC-Chain dưới dạng giá trị băm;
- Ghi mã tham chiếu giao dịch chuyển đổi và trạng thái vòng đời (yêu cầu, phê duyệt, hoàn tất, hủy) qua ConversionGateway;

- Ghi bằng chứng cảnh báo giám sát (vượt ngưỡng giao dịch, mẫu bất thường, trạng thái tuân thủ bất thường) lên DNC-Chain;

- Cung cấp giao diện giám sát on-chain cho cơ quan quản lý truy vấn theo thời gian thực phục vụ quản lý, giám sát, thanh tra, hậu kiểm.

Các chức năng nghiệp vụ khác (đăng ký tài khoản, xác minh định danh, khớp lệnh, chuyển đổi, thanh toán) do doanh nghiệp vận hành theo cơ chế sandbox và không thuộc phạm vi đặc tả Phụ lục I.

3. Kiến trúc kỹ thuật đặc thù

Nền tảng nghiệp vụ sandbox vận hành độc lập với DNC-Chain. SP8 chỉ có 03 cấu phần giao tiếp với DNC-Chain phục vụ chức năng quản lý nhà nước.

Bảng C.9.1. Ba cấu phần của SP8 giao tiếp với DNC-Chain

Cấu phần	Vị trí vận hành	Chức năng kỹ thuật chính
Compliance Bridge	Tại hạ tầng của doanh nghiệp vận hành thử nghiệm	Tính giá trị băm báo cáo tuân thủ định kỳ (KYC tổng hợp, AML/CFT, giao dịch theo ngưỡng); ký số; gửi lên ProofRegistry của Mô đun 2; không gửi dữ liệu cá nhân
Transaction Trace Connector	Tại hạ tầng của doanh nghiệp vận hành thử nghiệm	Liên kết mã tham chiếu giao dịch chuyển đổi với ConversionGateway của Mô đun 4; ghi trạng thái yêu cầu và trạng thái hoàn tất; không ghi giá trị giao dịch cụ thể hoặc định danh người dùng
Monitoring Endpoint	Giao tiếp giữa doanh nghiệp và cơ quan quản lý	Cung cấp giao diện để cơ quan quản lý truy vấn dữ liệu giám sát on-chain theo thời gian thực; kiểm soát quyền truy cập qua AccessGate của Mô đun 6

Ba loại dữ liệu duy nhất SP8 ghi lên DNC-Chain: (i) bằng chứng báo cáo tuân thủ định kỳ qua Compliance Bridge → ProofRegistry; (ii) mã tham chiếu giao dịch chuyển đổi qua Transaction Trace Connector → ConversionGateway; (iii) bằng chứng cảnh báo giám sát qua Compliance Bridge → ProofRegistry. Danh sách trường loại trừ không được ghi lên chuỗi gồm: họ tên, số định danh cá nhân, số hộ chiếu, ngày sinh, địa chỉ, quốc tịch, dữ liệu sinh trắc học của người dùng; số tài khoản ngân hàng, địa chỉ ví tài sản mã hoá; số dư tài khoản, số dư ví; giá trị giao dịch cụ thể (VND, USD, BTC, USDT), tỷ giá áp dụng; nội dung chi tiết hồ sơ KYC, ảnh giấy tờ, video eKYC; danh tính cán bộ KYC, AML/CFT của doanh nghiệp; báo cáo tài chính chi tiết, biên lợi nhuận doanh nghiệp; nội dung chi tiết giao dịch đáng ngờ.

Luồng kỹ thuật cơ bản: (i) đối với báo cáo tuân thủ, nền tảng sandbox kết xuất báo cáo theo chu kỳ đăng ký (dữ liệu báo cáo không rời khỏi hạ tầng doanh nghiệp); Compliance Bridge tính SHA-256, ký số ERC-191, gọi recordProof() của ProofRegistry;

trả biên lai xác minh cho doanh nghiệp; (ii) đối với giao dịch chuyển đổi, nền tảng phát sinh yêu cầu và phê duyệt theo quy trình nội bộ (chi tiết giao dịch lưu tại doanh nghiệp); Transaction Trace Connector sinh mã tham chiếu giao dịch (không trùng với mã người dùng), ghi trạng thái "yêu cầu" qua ConversionGateway; sau khi thực hiện xong, ghi trạng thái "hoàn tất" hoặc "hủy"; (iii) đối với truy vấn giám sát, cán bộ cơ quan quản lý có ROLE_SANDBOX_REGULATOR đăng nhập Monitoring Endpoint; AccessGate kiểm tra quyền; hệ thống truy vấn ProofRegistry và ConversionGateway, trả kết quả tổng hợp và cho phép xuất báo cáo.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP8: M1: -; M2: - (không sử dụng đầy đủ, chỉ recordProof()); M3: TC; **M4: TC (cơ chế riêng, chỉ ConversionGateway)**; M5: TC; M6: TC; M7: TC. SP8 không sử dụng bất kỳ mô đun nào ở mức bắt buộc.

- **Mô đun 4 (tùy chọn, cơ chế riêng):** Transaction Trace Connector liên kết mã tham chiếu giao dịch với ConversionGateway của Mô đun 4. Các hợp đồng còn lại của Mô đun 4 (TokenFactory, TokenRegistry, ComplianceEngine ở dạng đầy đủ, TokenLedger) **không được SP8 sử dụng** do SP8 không phát hành token trên DNC-Chain.

- **Mô đun 2 (không sử dụng ở dạng đầy đủ):** Compliance Bridge chỉ gọi hàm recordProof() của ProofRegistry để ghi giá trị băm báo cáo. Không sử dụng BatchManager, IssuerRegistry, VerificationLog, RevocationList ở dạng đầy đủ do bản chất sandbox không cần gom lô hoặc đăng ký nhà phát hành.

- **Mô đun 3 (tùy chọn):** doanh nghiệp vận hành được cấp khóa ký số qua KeyRegistry và cấp vai trò ROLE_SANDBOX_OPERATOR; cơ quan quản lý được cấp vai trò ROLE_SANDBOX_REGULATOR.

- **Mô đun 5 (tùy chọn):** ConversionGateway được Mô đun 5 quản lý vòng đời tương tự các hợp đồng khác của Mô đun 4.

- **Mô đun 6 (tùy chọn):** Monitoring Endpoint sử dụng AccessGate của Mô đun 6 để kiểm soát quyền truy cập của cơ quan quản lý.

- **Mô đun 7 (tùy chọn):** không sử dụng Hub ID cho người dùng cuối của SP8 (KYC người dùng thuộc doanh nghiệp vận hành theo cơ chế sandbox); chỉ áp dụng Hub ID đối với cán bộ cơ quan quản lý khi truy vấn dữ liệu giám sát.

Mô đun 1 không sử dụng. SP8 không kết nối liên chuỗi qua DNC-Chain.

5. Giao diện và tích hợp

SP8 **không kết nối trực tiếp với hệ thống nguồn theo mô hình LGSP** như các sản phẩm Tầng 1 và Tầng 2 do nền tảng nghiệp vụ vận hành độc lập theo cơ chế sandbox. Tích hợp chỉ diễn ra giữa 03 cầu phân giao tiếp với DNC-Chain và các hệ thống tương ứng.

Bảng C.9.2. Giao diện kỹ thuật chính của SP8

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Nền tảng nghiệp vụ sandbox với Compliance Bridge	REST trên HTTPS	mTLS + JWT + chữ ký số ERC-191 của doanh nghiệp
Nền tảng nghiệp vụ sandbox với Transaction Trace Connector	JSON-RPC	mTLS + JWT + chữ ký số của doanh nghiệp
Cơ quan quản lý với Monitoring Endpoint	REST + GraphQL qua AccessGate của Mô đun 6	mTLS + JWT + chữ ký số cơ quan + ROLE_SANDBOX_REGULATOR

Chuẩn kỹ thuật cốt lõi: ECDSA secp256k1 theo ERC-191 cho chữ ký số; HSM đạt quy chuẩn tương đương FIPS 140-3 Level 3 theo yêu cầu tại Phần A Mục VII; SHA-256 cho nội dung báo cáo; keccak256 cho mã tham chiếu giao dịch (độ dài 32 byte, sinh bằng keccak256 của mã nội bộ và dấu thời gian, không trùng với mã người dùng); RFC 3161 cho dấu thời gian. Các chuẩn mật mã chung áp dụng theo quy định tại Phần A Mục VII.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.9.3. Chỉ tiêu mức dịch vụ cốt lõi của 03 cấu phần SP8 giao tiếp với DNC-Chain

Chỉ tiêu	Mức cam kết
Thời gian ghi bằng chứng báo cáo tuân thủ định kỳ	≤ 60 phút với báo cáo tổng hợp; ≤ 5 phút với cảnh báo giám sát
Thời gian ghi mã tham chiếu giao dịch lên ConversionGateway	≤ 30 giây với 99% giao dịch
Thời gian phản hồi truy vấn tại Monitoring Endpoint	≤ 2 giây với 99,5% yêu cầu
Tỷ lệ ghi mã tham chiếu giao dịch thành công	≥ 99,9% tính theo tháng
Thời gian sẵn sàng của Transaction Trace Connector và Monitoring Endpoint	≥ 99,9% tính theo tháng

Chỉ tiêu thời gian phục hồi sau sự cố (RTO ≤ 4 giờ) và mất dữ liệu tối đa cho phép (RPO ≤ 15 phút với bằng chứng tuân thủ, ≤ 5 phút với mã tham chiếu giao dịch) áp dụng theo quy định chung tại Phần A Mục VII.

7. Điều kiện triển khai và giới hạn phạm vi đặc tả

Điều kiện kỹ thuật triển khai 03 cấu phần SP8 giao tiếp với DNC-Chain:

- Doanh nghiệp vận hành thử nghiệm đã được cấp phép theo Nghị quyết số 55/2024/NQ-HĐND và Quyết định số 1181/QĐ-UBND, triển khai trong phạm vi không gian theo Khoản 1 Điều 1 Nghị quyết số 55/2024/NQ-HĐND;

- Doanh nghiệp vận hành đã đăng ký khóa ký số vào KeyRegistry của Mô đun 3 và được cấp vai trò ROLE_SANDBOX_OPERATOR;

- Cơ quan quản lý theo pháp luật chuyên ngành đã được cấp vai trò ROLE_SANDBOX_REGULATOR với phạm vi truy vấn phù hợp;

- Nền tảng nghiệp vụ sandbox của doanh nghiệp vận hành đã thiết lập cơ chế phân loại giao dịch theo quy mô (theo nguyên tắc tương đương Thông tư số 50/2024/TT-NHNN của Ngân hàng Nhà nước về an toàn, bảo mật cho việc cung cấp dịch vụ trực tuyến trong ngành Ngân hàng) và áp dụng các hình thức xác nhận giao dịch tương ứng (mật khẩu, OTP, sinh trắc học qua VNeID Mức 2, chữ ký số) trên hợp đồng thông minh phục vụ chuyển đổi nhằm phòng, chống gian lận, lừa đảo; cơ chế này thuộc trách nhiệm của doanh nghiệp vận hành sandbox theo pháp luật ngành Ngân hàng, không thuộc phạm vi DNC-Chain;

- Quy trình chuyển đổi tài sản mã hóa sang đồng Việt Nam tại điểm chấp nhận thanh toán tuân thủ Nghị định số 52/2024/NĐ-CP của Chính phủ về thanh toán không dùng tiền mặt: tài sản mã hóa được chuyển đổi sang đồng Việt Nam trước khi thực hiện thanh toán cho điểm chấp nhận thông qua tài khoản thanh toán hợp pháp; điểm chấp nhận chỉ nhận đồng Việt Nam; SP8 không cấu thành phương tiện thanh toán mới;

- Compliance Bridge, Transaction Trace Connector, Monitoring Endpoint đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;

- Cơ chế phối hợp giữa các cơ quan quản lý liên quan đã được xác lập bằng văn bản;

- Lược đồ báo cáo tuân thủ định kỳ đã được cơ quan quản lý phê duyệt và đăng ký với Compliance Bridge.

Giới hạn phạm vi đặc tả đối với SP8. Phụ lục I không đặc tả các nội dung sau vì thuộc cơ chế riêng của sandbox, thẩm quyền của cơ quan quản lý chuyên ngành và trách nhiệm của doanh nghiệp vận hành:

- Kiến trúc kỹ thuật nội bộ của nền tảng nghiệp vụ sandbox (ví tài sản mã hóa, sổ lệnh, khớp lệnh, cổng kết nối ngân hàng, cổng thanh toán, QR thanh toán, hệ thống nạp và rút);

- Quy trình xác minh định danh điện tử (eKYC), phân loại khách hàng, hạn mức giao dịch theo khách hàng, quy trình AML/CFT chi tiết và Travel Rule;

- Cơ chế quản lý ví lưu ký (custody), quản lý khoá riêng của người dùng, cơ chế bảo vệ tài sản, cơ chế giải quyết tranh chấp, cơ chế đền bù rủi ro;

- Tham số nghiệp vụ của thử nghiệm (phí giao dịch, tỷ giá chuyển đổi, thời gian xử lý nghiệp vụ nội bộ, các hạn mức);

- Chi tiết nghĩa vụ kế toán, nghĩa vụ thuế, báo cáo tài chính của doanh nghiệp vận hành theo pháp luật chuyên ngành;

- Danh sách tài sản mã hoá được phép chuyển đổi, tiêu chí lựa chọn loại tài sản, điều kiện niêm yết;
- Cơ chế tuân thủ pháp luật chuyên ngành về ngân hàng, ngoại hối, phòng chống rửa tiền, phòng chống tài trợ khủng bố.

SP9 - Nền tảng phát hành, lưu ký và giao dịch tài sản mã hoá (RWA)

1. Định vị sản phẩm

SP9 thuộc Tầng 4 của Đề án, gắn với Trung tâm tài chính quốc tế (IFC) tại Việt Nam theo Nghị quyết số 222/2025/QH15 của Quốc hội và Nghị định số 323/2025/NĐ-CP hướng dẫn thi hành. SP9 không phải ứng dụng công dùng chung của thành phố; Đề án thực hiện vai trò tiếp nhận, định vị và điều phối ở cấp thành phố, không thay thế cơ chế riêng và pháp luật chuyên ngành.

Bản chất SP9 là nền tảng nghiệp vụ do doanh nghiệp, tổ chức có nhu cầu phát hành tài sản mã hoá có tài sản tham chiếu xây dựng và vận hành theo cơ chế có kiểm soát, gắn với phạm vi thí điểm được cơ quan có thẩm quyền cho phép. Các tài sản tham chiếu bao gồm bất động sản, hạ tầng, trái phiếu đô thị, tài sản khác được pháp luật cho phép. Phụ lục I chỉ đặc tả 04 cấu phần giao tiếp với DNC-Chain thuộc phần công vụ; phần thương mại của nền tảng nghiệp vụ do doanh nghiệp đầu tư, không thuộc phạm vi Phụ lục.

SP9 sử dụng ERC-1400 là chuẩn chính thức cho Token đại diện quyền lợi kinh tế gắn với tài sản thực, thống nhất với Bảng 4.2 Phần B (nhóm Token đại diện tài sản có thể chuyển nhượng có kiểm soát). SP9 không triển khai hợp đồng thông minh riêng trên DNC-Chain; Token RWA nghiệp vụ được đúc và quản lý trên nền tảng nghiệp vụ theo ERC-1400 trên hạ tầng blockchain phù hợp của nền tảng đó; DNC-Chain chỉ nhận mã tham chiếu phục vụ giám sát.

2. Chức năng nghiệp vụ chính

Phạm vi chức năng thuộc Phụ lục I (chỉ 04 cấu phần giao tiếp với DNC-Chain):

- Ghi bằng chứng hồ sơ pháp lý tài sản gốc (hash hồ sơ, loại tài sản, mã tài sản đã băm);
- Ghi mã tham chiếu đợt phát hành và mã Token RWA vào TokenRegistry của Mô đun 4;
- Ghi mã tham chiếu giao dịch lưu ký và giao dịch thứ cấp có kiểm soát;
- Ghi bằng chứng báo cáo tuân thủ và cảnh báo giám sát (KYC nhà đầu tư tổng hợp, AML/CFT, giao dịch theo ngưỡng, giám sát phân loại nhà đầu tư);
- Cung cấp giao diện giám sát on-chain cho cơ quan quản lý theo pháp luật chuyên ngành về tài chính, ngân hàng, chứng khoán.

3. Kiến trúc kỹ thuật đặc thù

Nền tảng nghiệp vụ RWA vận hành trên kiến trúc kỹ thuật hoặc hạ tầng blockchain phù hợp với mô hình triển khai cụ thể; không bắt buộc toàn bộ nghiệp vụ vận hành trực tiếp trên DNC-Chain. SP9 có 04 cấu phần giao tiếp với DNC-Chain.

Bảng C.10.1. Bốn cấu phần của SP9 giao tiếp với DNC-Chain

Cấu phần	Vị trí vận hành	Chức năng kỹ thuật chính
Asset Reference Proof Bridge	Tại hạ tầng của doanh nghiệp vận hành nền tảng	Tính SHA-256 hồ sơ pháp lý tài sản gốc; ghi bằng chứng lên ProofRegistry của Mô đun 2; không ghi nội dung hồ sơ pháp lý
Tokenization Registry Connector	Tại hạ tầng của doanh nghiệp vận hành nền tảng	Ghi mã tham chiếu đợt phát hành, mã Token RWA, mã tham chiếu giao dịch phát hành và lưu ký vào TokenRegistry của Mô đun 4; không ghi giá trị giao dịch cụ thể
Compliance and Surveillance Bridge	Tại hạ tầng của doanh nghiệp vận hành nền tảng	Gửi bằng chứng báo cáo tuân thủ, AML/CFT, phòng chống rửa tiền và tài trợ khủng bố, trạng thái cảnh báo giám sát lên ProofRegistry của Mô đun 2
Regulatory Monitoring Endpoint	Giao tiếp giữa doanh nghiệp và cơ quan quản lý	Cung cấp giao diện cho các cơ quan có thẩm quyền truy vấn dữ liệu giám sát on-chain theo thời gian thực; kiểm soát quyền truy cập qua AccessGate của Mô đun 6

Bốn loại dữ liệu duy nhất SP9 ghi lên DNC-Chain: (i) bằng chứng hồ sơ pháp lý tài sản gốc qua Asset Reference Proof Bridge → ProofRegistry; (ii) mã tham chiếu đợt phát hành và Token RWA qua Tokenization Registry Connector → TokenRegistry; (iii) mã tham chiếu giao dịch lưu ký và giao dịch thứ cấp có kiểm soát qua Tokenization Registry Connector; (iv) bằng chứng báo cáo tuân thủ và cảnh báo giám sát qua Compliance and Surveillance Bridge → ProofRegistry. Danh sách trường loại trừ không được ghi lên chuỗi gồm: họ tên, số định danh cá nhân, số hộ chiếu, ngày sinh, địa chỉ, quốc tịch, dữ liệu sinh trắc học của nhà đầu tư; số tài khoản ngân hàng, số tài khoản chứng khoán, địa chỉ ví; số dư tài khoản, số dư ví, số lượng token nắm giữ của từng nhà đầu tư; giá trị giao dịch cụ thể (giá phát hành, giá thứ cấp, giá tất toán); nội dung chi tiết hồ sơ pháp lý tài sản gốc (hợp đồng mua bán, giấy chứng nhận quyền sử dụng đất, bản vẽ kỹ thuật, báo cáo định giá); báo cáo tài chính chi tiết; hồ sơ KYC nhà đầu tư; danh tính cán bộ KYC, AML/CFT, quản lý rủi ro; nội dung giao dịch đáng ngờ; điều khoản thương mại chi tiết của hợp đồng phát hành và lưu ký.

Luồng kỹ thuật cơ bản: (i) đối với hồ sơ pháp lý tài sản gốc, cơ quan tư pháp và cơ quan quản lý chuyên ngành xác nhận tính pháp lý của tài sản theo pháp luật chuyên ngành; nền tảng nghiệp vụ kết tập hồ sơ, tính SHA-256 tại hạ tầng doanh nghiệp; Asset Reference Proof Bridge ghi bằng chứng qua ProofRegistry; (ii) đối với đúc Token RWA, nền tảng nghiệp vụ hoàn tất phê duyệt phát hành theo pháp luật chuyên ngành, đúc Token theo ERC-1400 trên hạ tầng nghiệp vụ (chi tiết phát hành lưu tại nền tảng); Tokenization Registry Connector ghi mã đợt phát hành và mã Token vào TokenRegistry dưới dạng bản ghi tham chiếu (không phải token nghiệp vụ thật); ghi liên kết với bằng chứng hồ sơ pháp lý tài sản gốc đã ghi trước đó; (iii) đối với giao dịch lưu ký và thứ cấp, nền tảng áp dụng

allowlist nhà đầu tư, phân loại nhà đầu tư theo pháp luật chuyên ngành; Tokenization Registry Connector sinh mã tham chiếu giao dịch, ghi các trạng thái "yêu cầu → hoàn tất / hủy / circuit breaker kích hoạt"; (iv) đối với truy vấn giám sát, cán bộ cơ quan quản lý đăng nhập Regulatory Monitoring Endpoint với ROLE_RWA_REGULATOR hoặc ROLE_RWA_AUDITOR; hệ thống truy vấn ProofRegistry và TokenRegistry, trả kết quả tổng hợp.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP9: M1: -; M2: - (không sử dụng đầy đủ, chỉ recordProof()); M3: TC; **M4: TC (cơ chế riêng)**; M5: TC; M6: TC; M7: TC.

- **Mô đun 4 (tùy chọn, cơ chế riêng):** Tokenization Registry Connector liên kết mã Token RWA với TokenRegistry. **TokenFactory không được SP9 sử dụng trực tiếp để đúc token** (token nghiệp vụ được đúc trên nền tảng nghiệp vụ); chỉ ghi mã tham chiếu phục vụ giám sát.

- **Mô đun 2 (không sử dụng ở dạng đầy đủ):** Asset Reference Proof Bridge và Compliance and Surveillance Bridge chỉ gọi recordProof() để ghi giá trị băm.

- **Mô đun 3 (tùy chọn):** doanh nghiệp vận hành được cấp vai trò ROLE_RWA_OPERATOR; bên lưu ký có ROLE_RWA_CUSTODIAN; cơ quan quản lý có ROLE_RWA_REGULATOR; cơ quan thanh tra, kiểm toán có ROLE_RWA_AUDITOR.

- **Mô đun 5 (tùy chọn):** các hợp đồng trên DNC-Chain liên quan tới SP9 (nếu có) được Mô đun 5 quản lý vòng đời.

- **Mô đun 6 (tùy chọn):** Regulatory Monitoring Endpoint sử dụng AccessGate của Mô đun 6.

- **Mô đun 7 (tùy chọn):** không sử dụng Hub ID cho nhà đầu tư cuối (do KYC nhà đầu tư do doanh nghiệp vận hành và bên lưu ký quản lý theo pháp luật chuyên ngành); chỉ áp dụng Hub ID đối với cán bộ cơ quan quản lý.

Mô đun 1 không sử dụng. Trường hợp có giao dịch liên chuỗi thuộc nền tảng nghiệp vụ, cơ chế liên chuỗi được xử lý tại chính nền tảng nghiệp vụ theo pháp luật chuyên ngành, không qua DNC-Chain.

SP9.5. Giao diện và tích hợp

SP9 không kết nối trực tiếp với hệ thống nguồn theo mô hình LGSP. Tích hợp chỉ diễn ra giữa 04 cầu phân giao tiếp với DNC-Chain và các hệ thống tương ứng.

Bảng C.10.2. Giao diện kỹ thuật chính của SP9

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
--------------------	-----------	----------------

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Nền tảng nghiệp vụ RWA với 03 bridge (Asset Reference, Tokenization Registry, Compliance and Surveillance)	REST trên HTTPS	mTLS + JWT + chữ ký số ERC-191 của doanh nghiệp
Cơ quan quản lý với Regulatory Monitoring Endpoint	REST + GraphQL qua AccessGate của Mô đun 6	mTLS + JWT + chữ ký số cơ quan + ROLE_RWA_REGULATOR hoặc ROLE_RWA_AUDITOR

Chuẩn kỹ thuật cốt lõi: ERC-1400 cho chuẩn token tham chiếu đăng ký tại TokenRegistry của Mô đun 4 (không đưa ERC-3643 vào đặc tả do xung đột nguyên lý với mô hình Hub ID của Mô đun 7); ECDSA secp256k1 theo ERC-191 cho chữ ký số; HSM đạt quy chuẩn tương đương FIPS 140-3 Level 3; SHA-256 cho nội dung hồ sơ và báo cáo; keccak256 cho mã tham chiếu giao dịch (độ dài 32 byte); RFC 3161 cho dấu thời gian. Các chuẩn mật mã chung áp dụng theo quy định tại Phần A Mục VII.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.10.3. Chỉ tiêu mức dịch vụ cốt lõi của 04 cấu phần SP9 giao tiếp với DNC-Chain

Chỉ tiêu	Mức cam kết
Thời gian ghi bằng chứng hồ sơ pháp lý tài sản gốc	≤ 60 giây với 99% bằng chứng
Thời gian ghi mã tham chiếu đợt phát hành và Token	≤ 30 giây với 99% đợt
Thời gian ghi mã tham chiếu giao dịch	≤ 15 giây với 99% giao dịch
Thời gian ghi bằng chứng báo cáo tuân thủ	≤ 60 phút với báo cáo tổng hợp; ≤ 5 phút với cảnh báo
Thời gian phản hồi truy vấn tại Regulatory Monitoring Endpoint	≤ 2 giây với 99,5% yêu cầu
Tỷ lệ ghi mã tham chiếu thành công	≥ 99,9% tính theo tháng

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút với bằng chứng, ≤ 5 phút với mã tham chiếu giao dịch) áp dụng theo quy định chung tại Phần A Mục VII.

7. Điều kiện triển khai và giới hạn phạm vi đặc tả

Điều kiện kỹ thuật triển khai 04 cấu phần SP9 giao tiếp với DNC-Chain:

- Doanh nghiệp vận hành nền tảng đã được cấp phép theo pháp luật chuyên ngành và khuôn khổ pháp lý áp dụng cho IFC (Nghị quyết số 222/2025/QH15, Nghị định số 323/2025/NĐ-CP);

- Cơ quan có thẩm quyền đã phối hợp với cơ quan tư pháp rà soát và xác định tính pháp lý của tài sản gốc, quyền sở hữu và quyền tài sản liên quan trước khi đưa vào hệ thống;

- Doanh nghiệp vận hành, bên lưu ký, cơ quan quản lý, cơ quan thanh tra đã được đăng ký khóa ký số và cấp các vai trò tương ứng trong AccessControlRegistry;

- Bốn cấu phần (Asset Reference Proof Bridge, Tokenization Registry Connector, Compliance and Surveillance Bridge, Regulatory Monitoring Endpoint) đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;

- Cơ chế phối hợp giữa các cơ quan quản lý có thẩm quyền theo pháp luật chuyên ngành về tài chính, ngân hàng, chứng khoán đã được xác lập bằng văn bản;

- Lược đồ báo cáo tuân thủ định kỳ đã được cơ quan quản lý phê duyệt và đăng ký với Compliance and Surveillance Bridge.

Giới hạn phạm vi đặc tả đối với SP9. Phụ lục I không đặc tả các nội dung sau vì thuộc cơ chế riêng gắn với IFC, thẩm quyền của cơ quan quản lý chuyên ngành và trách nhiệm của doanh nghiệp vận hành:

- Kiến trúc kỹ thuật nội bộ của nền tảng nghiệp vụ phát hành (cơ chế đúc token nghiệp vụ, sổ lệnh, khớp lệnh giao dịch thứ cấp, cơ chế ký quỹ, cơ chế thanh toán, cơ chế tất toán);

- Quy trình phê duyệt phát hành, hồ sơ chào bán, công bố thông tin, quảng bá đợt phát hành;

- Quy trình thẩm định dự án, phân loại nhà đầu tư (chuyên nghiệp, đại chúng, tổ chức), hạn mức đầu tư theo nhóm, quy trình AML/CFT chi tiết và Travel Rule;

- Cơ chế quản lý bên lưu ký (custody), quản lý khoá, quản lý tài sản tham chiếu, cơ chế chuyển giao tài sản khi tất toán;

- Cơ chế quản lý quỹ, giải quyết tranh chấp, bảo vệ nhà đầu tư, đền bù rủi ro, bảo hiểm trách nhiệm;

- Tham số nghiệp vụ (phí phát hành, phí lưu ký, phí giao dịch thứ cấp, hoa hồng, lãi suất, chi phí phục vụ);

- Chi tiết nghĩa vụ kế toán, nghĩa vụ thuế, báo cáo tài chính của doanh nghiệp phát hành và doanh nghiệp vận hành theo pháp luật chuyên ngành;

- Tiêu chí lựa chọn loại tài sản được phép token hoá, quy định về thẩm định giá tài sản tham chiếu;

- Cơ chế tuân thủ pháp luật chuyên ngành về chứng khoán, ngoại hối, phòng chống rửa tiền, phòng chống tài trợ khủng bố.

SP10 - Nền tảng gọi vốn cộng đồng trên blockchain

1. Định vị sản phẩm

SP10 thuộc Tầng 4 của Đề án, gắn với IFC Đà Nẵng theo Nghị quyết số 222/2025/QH15 của Quốc hội và Nghị định số 323/2025/NĐ-CP hướng dẫn thi hành. SP10 không phải ứng dụng công dùng chung của thành phố; Đề án thực hiện vai trò tiếp nhận, định vị và điều phối ở cấp thành phố.

Bản chất SP10 là nền tảng gọi vốn cộng đồng có kiểm soát, phục vụ các dự án khởi nghiệp sáng tạo và các doanh nghiệp trong phạm vi phù hợp, trọng tâm vào cam kết góp vốn, giám sát giải ngân theo mốc và kiểm soát rủi ro. SP10 được triển khai theo ba nhóm mô hình: gọi vốn theo phần thưởng; tài trợ hoặc đóng góp cộng đồng; các mô hình có tính chất đầu tư. Đối với các mô hình có liên quan tài sản số, tài sản mã hoá, giao dịch số hoặc có yếu tố phân chia lợi ích tài chính, việc triển khai chỉ xem xét trong phạm vi pháp luật hiện hành, cơ chế sandbox hoặc theo quyết định của cơ quan có thẩm quyền. Phụ lục I chỉ đặc tả 04 cấu phần giao tiếp với DNC-Chain; phần thương mại do doanh nghiệp đầu tư.

SP10 không triển khai hợp đồng thông minh riêng trên DNC-Chain; token (nếu có, với mô hình có yếu tố đầu tư) được đúc trên nền tảng nghiệp vụ; DNC-Chain chỉ nhận mã tham chiếu phục vụ giám sát.

2. Chức năng nghiệp vụ chính

Phạm vi chức năng thuộc Phụ lục I (chỉ 04 cấu phần giao tiếp với DNC-Chain):

- Ghi bằng chứng hồ sơ dự án đã thẩm định và phương án gọi vốn, phương án giải ngân theo mốc;

- Ghi mã tham chiếu cam kết góp vốn và trạng thái vòng đời (đăng ký, xác nhận, hủy);

- Ghi mã tham chiếu mốc giải ngân và trạng thái xác nhận (chưa xác nhận, đã xác nhận, bị phản đối, bị phủ quyết) cùng trạng thái giải ngân (chưa giải ngân, đã giải ngân, tạm dừng, circuit breaker);

- Ghi bằng chứng báo cáo tuân thủ (AML/CFT đối với mô hình có yếu tố tài chính, báo cáo tiến độ dự án) và cảnh báo giám sát;

- Cung cấp giao diện giám sát on-chain cho cơ quan quản lý theo pháp luật chuyên ngành về chứng khoán, thị trường vốn.

3. Kiến trúc kỹ thuật đặc thù

Kiến trúc SP10 tương tự SP9: nền tảng nghiệp vụ vận hành trên kiến trúc kỹ thuật hoặc blockchain phù hợp với mô hình triển khai cụ thể; không bắt buộc toàn bộ nghiệp vụ vận hành trực tiếp trên DNC-Chain. SP10 có 04 cấu phần giao tiếp với DNC-Chain.

Bảng C.11.1. Bốn cấu phần của SP10 giao tiếp với DNC-Chain

Cấu phần	Vị trí vận hành	Chức năng kỹ thuật chính
Project Proof Bridge	Tại hạ tầng của doanh nghiệp vận hành nền tảng	Tính SHA-256 hồ sơ dự án đã thẩm định, phương án gọi vốn, phương án giải ngân; ghi lên ProofRegistry của Mô đun 2; không ghi nội dung hồ sơ chi tiết
Commitment and Milestone Connector	Tại hạ tầng của doanh nghiệp vận hành nền tảng	Ghi mã tham chiếu cam kết góp vốn, mã tham chiếu mốc giải ngân, trạng thái xác nhận mốc, trạng thái giải ngân qua ProofRegistry của Mô đun 2 và TokenRegistry của Mô đun 4 (khi áp dụng mô hình có token)
Compliance and Surveillance Bridge	Tại hạ tầng của doanh nghiệp vận hành nền tảng	Gửi bằng chứng báo cáo tuân thủ, AML/CFT (đối với mô hình có yếu tố tài chính), trạng thái cảnh báo giám sát, trạng thái circuit breaker giải ngân lên ProofRegistry
Regulatory Monitoring Endpoint	Giao tiếp giữa doanh nghiệp và cơ quan quản lý	Cung cấp giao diện cho các cơ quan có thẩm quyền truy vấn dữ liệu giám sát on-chain; kiểm soát quyền truy cập qua AccessGate của Mô đun 6

Bốn loại dữ liệu duy nhất SP10 ghi lên DNC-Chain tương ứng với bốn cấu phần trên. Danh sách trường loại trừ không được ghi lên chuỗi gồm: họ tên, số định danh cá nhân, số hộ chiếu, ngày sinh, địa chỉ, quốc tịch của nhà đầu tư và chủ dự án; số tài khoản ngân hàng, địa chỉ ví; số dư tài khoản, số dư ví, số lượng cam kết của từng nhà đầu tư; giá trị cam kết góp vốn cụ thể; giá trị giải ngân cụ thể theo từng mốc; nội dung chi tiết hồ sơ dự án (kế hoạch kinh doanh, phân tích thị trường, dự toán tài chính, hợp đồng thương mại); báo cáo tài chính của chủ dự án và doanh nghiệp vận hành; hồ sơ KYC nhà đầu tư; danh tính cán bộ KYC, AML/CFT, thẩm định dự án; nội dung giao dịch đáng ngờ; điều khoản thương mại chi tiết của hợp đồng gọi vốn.

Luồng kỹ thuật cơ bản: (i) đối với bằng chứng hồ sơ dự án, doanh nghiệp vận hành và cơ quan có thẩm quyền thẩm định và phê duyệt hồ sơ theo pháp luật chuyên ngành; nền tảng nghiệp vụ kết tập hồ sơ, tính SHA-256; Project Proof Bridge gọi recordProof() qua ProofRegistry; (ii) đối với cam kết góp vốn, nhà đầu tư đăng ký qua cổng được cấp phép, xác minh KYC và tư cách nhà đầu tư theo pháp luật chuyên ngành (chi tiết cam kết lưu tại doanh nghiệp); Commitment and Milestone Connector sinh mã tham chiếu, ghi trạng thái "đăng ký → xác nhận / hủy"; (iii) đối với mốc giải ngân, chủ dự án hoàn thành công việc theo mốc đã phê duyệt và gửi báo cáo; cơ quan xác nhận mốc có ROLE_MILESTONE_VERIFIER thẩm định và xác nhận theo thẩm quyền; Commitment and Milestone Connector ghi trạng thái "đã xác nhận → đã giải ngân"; trường hợp phát hiện vi phạm, cơ quan có thẩm quyền yêu cầu dừng giải ngân và hệ thống ghi trạng thái "circuit breaker kích hoạt"; (iv) đối với truy vấn giám sát, cán bộ cơ quan quản lý với

ROLE_CROWDFUNDING_REGULATOR hoặc
ROLE_CROWDFUNDING_AUDITOR truy vấn qua Regulatory Monitoring Endpoint.

4. Phụ thuộc mô đun

Theo Bảng B.8.1 Phần B, mức phụ thuộc của SP10: M1: -; M2: - (không sử dụng đầy đủ, chỉ recordProof()); M3: TC; **M4: TC (cơ chế riêng)**; M5: TC; M6: TC; M7: TC.

- **Mô đun 4 (tùy chọn, cơ chế riêng):** Commitment and Milestone Connector liên kết mã tham chiếu cam kết và mốc giải ngân với TokenRegistry đối với mô hình có yếu tố token. **TokenFactory không được SP10 sử dụng trực tiếp để đúc token** (token được đúc tại nền tảng nghiệp vụ khi áp dụng).

- **Mô đun 2 (không sử dụng ở dạng đầy đủ):** Project Proof Bridge và Compliance and Surveillance Bridge chỉ gọi recordProof().

- **Mô đun 3 (tùy chọn):** các vai trò ROLE_CROWDFUNDING_OPERATOR (doanh nghiệp vận hành), ROLE_PROJECT_OWNER (chủ dự án), ROLE_MILESTONE_VERIFIER (cơ quan xác nhận mốc), ROLE_CROWDFUNDING_REGULATOR (cơ quan quản lý), ROLE_CROWDFUNDING_AUDITOR (thanh tra, kiểm toán).

- **Mô đun 5, Mô đun 6 (tùy chọn):** tương tự SP9.

- **Mô đun 7 (tùy chọn):** không sử dụng Hub ID cho nhà đầu tư cuối; chỉ áp dụng Hub ID đối với cán bộ cơ quan quản lý.

Mô đun 1 không sử dụng. SP10 không kết nối liên chuỗi qua DNC-Chain; trường hợp có yếu tố liên chuỗi thuộc nền tảng nghiệp vụ, được xử lý tại chính nền tảng nghiệp vụ theo pháp luật chuyên ngành.

5. Giao diện và tích hợp

SP10 không kết nối trực tiếp với hệ thống nguồn theo mô hình LGSP. Tích hợp chỉ diễn ra giữa 04 cầu phân giao tiếp với DNC-Chain.

Bảng C.11.2. Giao diện kỹ thuật chính của SP10

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Nền tảng nghiệp vụ với 03 bridge (Project Proof, Commitment and Milestone, Compliance and Surveillance)	REST trên HTTPS	mTLS + JWT + chữ ký số ERC-191 của doanh nghiệp
Cơ quan xác nhận mốc	Giao diện ký số xác nhận mốc trên Commitment and Milestone Connector	mTLS + JWT + chữ ký số cơ quan + ROLE_MILESTONE_VERIFIER

Đối tượng tích hợp	Giao diện	Chuẩn xác minh
Cơ quan quản lý với Regulatory Monitoring Endpoint	REST + GraphQL qua AccessGate của Mô đun 6	mTLS + JWT + chữ ký số cơ quan + ROLE_CROWDFUNDING_REGULATOR hoặc ROLE_CROWDFUNDING_AUDITOR

Chuẩn kỹ thuật cốt lõi: ECDSA secp256k1 theo ERC-191 cho chữ ký số; HSM đạt quy chuẩn tương đương FIPS 140-3 Level 3; SHA-256 cho nội dung hồ sơ và báo cáo; keccak256 cho mã tham chiếu (độ dài 32 byte, không trùng với mã nhà đầu tư); RFC 3161 cho dấu thời gian. Các chuẩn mật mã chung áp dụng theo quy định tại Phần A Mục VII. Ràng buộc nghiệp vụ quan trọng: mỗi dự án phải có tối thiểu 02 mốc giải ngân, cho phép giám sát theo mốc, không giải ngân một lần toàn bộ.

6. Chỉ tiêu kỹ thuật cốt lõi

Bảng C.11.3. Chỉ tiêu mức dịch vụ cốt lõi của 04 cấu phần SP10 giao tiếp với DNC-Chain

Chỉ tiêu	Mức cam kết
Thời gian ghi bằng chứng hồ sơ dự án	≤ 60 giây với 99% bằng chứng
Thời gian ghi mã tham chiếu cam kết góp vốn	≤ 15 giây với 99% cam kết
Thời gian ghi trạng thái mốc giải ngân sau khi cơ quan xác nhận	≤ 30 giây với 99% mốc
Thời gian ghi bằng chứng báo cáo tuân thủ	≤ 60 phút với báo cáo tổng hợp; ≤ 5 phút với cảnh báo
Thời gian phản hồi truy vấn tại Regulatory Monitoring Endpoint	≤ 2 giây với 99,5% yêu cầu
Tỷ lệ ghi mã tham chiếu thành công	$\geq 99,9\%$ tính theo tháng

Chỉ tiêu thời gian phục hồi sau sự cố ($RTO \leq 4$ giờ) và mất dữ liệu tối đa cho phép ($RPO \leq 15$ phút với bằng chứng, ≤ 5 phút với mã tham chiếu cam kết và mốc) áp dụng theo quy định chung tại Phần A Mục VII.

7. Điều kiện triển khai và giới hạn phạm vi đặc tả

Điều kiện kỹ thuật triển khai 04 cấu phần SP10 giao tiếp với DNC-Chain:

- Doanh nghiệp vận hành nền tảng đã được cấp phép theo cơ chế sandbox hoặc theo pháp luật chuyên ngành;

- Dự án gọi vốn đã được thẩm định và phê duyệt theo pháp luật chuyên ngành trước khi ghi bằng chứng;

- Doanh nghiệp vận hành, chủ dự án, cơ quan xác nhận mốc, cơ quan quản lý, cơ quan thanh tra đã được đăng ký khóa ký số và cấp vai trò tương ứng trong AccessControlRegistry;

- Bốn cầu phần (Project Proof Bridge, Commitment and Milestone Connector, Compliance and Surveillance Bridge, Regulatory Monitoring Endpoint) đã hoàn thành kiểm toán bảo mật độc lập theo quy định tại Phần A Mục XII;

- Cơ chế phối hợp giữa các cơ quan quản lý có thẩm quyền theo pháp luật chuyên ngành về chứng khoán, thị trường vốn đã được xác lập bằng văn bản; đối với mô hình SP10 có liên quan đến hoạt động cung cấp dịch vụ về chứng khoán, có văn bản chấp thuận của Ủy ban Chứng khoán Nhà nước theo Khoản 4 Điều 12 Luật Chứng khoán số 54/2019/QH14 (sửa đổi, bổ sung bởi Luật số 56/2024/QH15);

- Lược đồ báo cáo tuân thủ đã được cơ quan quản lý phê duyệt và đăng ký với Compliance and Surveillance Bridge.

Giới hạn phạm vi đặc tả đối với SP10. Phụ lục I không đặc tả các nội dung sau vì thuộc cơ chế riêng gắn với IFC, thẩm quyền của cơ quan quản lý chuyên ngành và trách nhiệm của doanh nghiệp vận hành:

- Kiến trúc kỹ thuật nội bộ của nền tảng nghiệp vụ (công đăng ký dự án, công đăng ký nhà đầu tư, cơ chế thẩm định tự động, cơ chế khớp cam kết, cơ chế đúc token khi áp dụng, cơ chế thanh toán, cơ chế giải ngân);

- Quy trình thẩm định dự án gọi vốn, tiêu chí phê duyệt, quy trình công bố thông tin dự án, quy trình quảng bá;

- Quy trình phân loại nhà đầu tư (đại chúng, chuyên nghiệp, tổ chức), hạn mức đầu tư theo nhóm;

- Quy trình AML/CFT chi tiết đối với mô hình có yếu tố tài chính;

- Cơ chế quản lý quỹ gọi vốn, ký quỹ, giải ngân cụ thể, hoàn vốn khi dự án không đủ vốn tối thiểu, hoàn vốn khi dự án vi phạm;

- Cơ chế giải quyết tranh chấp giữa nhà đầu tư và chủ dự án, bảo vệ nhà đầu tư, đền bù rủi ro;

- Tham số nghiệp vụ (phí đăng ký dự án, phí nền tảng, phí giải ngân, hoa hồng, tỷ lệ phần thưởng theo mô hình phần thưởng);

- Chi tiết nghĩa vụ kế toán, nghĩa vụ thuế, báo cáo tài chính của chủ dự án và doanh nghiệp vận hành theo pháp luật chuyên ngành;

- Cơ chế tuân thủ pháp luật chuyên ngành về chứng khoán, thị trường vốn, phòng chống rửa tiền, phòng chống tài trợ khủng bố;

- Tiêu chí lựa chọn loại dự án được phép gọi vốn, quy mô vốn tối đa cho phép theo từng mô hình

Phụ lục II
DỰ TOÁN KINH PHÍ

Tổng nhu cầu kinh phí thực hiện Đề án là **268, 0 tỷ đồng**, gồm ngân sách địa phương **182,49 tỷ đồng (68,09%)** và nguồn ngoài ngân sách (doanh nghiệp, hợp tác công - tư, xã hội hoá, nguồn hợp pháp khác) **85,51 tỷ đồng (31,91%)**.

Cơ cấu được trình bày tại **02 bảng**: Bảng A.1 tóm tắt theo hợp phần; Bảng A.2 chi tiết theo hạng mục.

Đơn vị tính: tỷ đồng.

Bảng A.1. Tổng hợp kinh phí theo hợp phần và theo năm giai đoạn 2026-2030

Mã	Hợp phần	Tổng	NSDP	Ngoài NS	2026	2027	2028	2029	2030
I	THẺ CHẾ VÀ KHUNG PHÁP LÝ	0,620	0,620	-	0,220	0,10	0,10	0,10	0,10
II	HẠ TẦNG BLOCKCHAIN DÙNG CHUNG (DNC-CHAIN)	62,80	39,00	23,80	53,80	2,00	2,50	2,50	2,00
III	TRIỂN KHAI 10 SẢN PHẨM THEO 04 TẦNG CẤP ĐỘ	151,40	89,69	61,71	25,80	25,50	34,90	33,50	31,70
IV	CHUẨN HOÁ DỮ LIỆU, TÍCH HỢP, BẢO ĐẢM AN TOÀN THÔNG TIN VÀ AN NINH MẠNG	5,00	5,00	-	1,60	1,10	1,10	0,60	0,60
V	NGUỒN NHÂN LỰC, NĂNG LỰC TRIỂN KHAI VÀ HỆ SINH THÁI	38,18	38,18	-	9,10	9,02	7,02	7,02	6,02
VI	DỰ PHÒNG	10,00	10,00	-	2,00	2,00	2,00	2,00	2,00
VII	TỔNG CỘNG	268,00	182,49	85,51	92,52	39,72	47,62	45,72	42,42

	Tỷ lệ %	100	68,09	31,91	34,52	14,82	17,77	17,06	15,83
--	---------	-----	-------	-------	-------	-------	-------	-------	-------

Bảng A.2. Chi tiết kinh phí theo hạng mục và theo năm giai đoạn 2026-2030

Mã	Tên hạng mục	Nguồn vốn	Tổng	2026	2027	2028	2029	2030
I	THẺ CHẾ VÀ KHUNG PHÁP LÝ	NSDP	0,62	0,220	0,10	0,10	0,10	0,10
1	Rà soát, hệ thống hóa văn bản pháp lý	NSDP	0,10	0,020	0,020	0,020	0,020	0,020
2	Quy chế quản trị, vận hành DNC-Chain và Quy chế vòng đời ứng dụng	NSDP	0,130	0,050	0,020	0,020	0,020	0,020
3	Bộ tiêu chuẩn, yêu cầu kết nối, chia sẻ và kiểm chứng dữ liệu	NSDP	0,130	0,050	0,020	0,020	0,020	0,020
4	Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án	NSDP	0,130	0,050	0,020	0,020	0,020	0,020
5	Quy chế bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân đối với DNC-Chain và các ứng dụng kết nối	NSDP	0,130	0,050	0,020	0,020	0,020	0,020
II	HẠ TẦNG BLOCKCHAIN (DNC-CHAIN)	Hỗn hợp	62,80	53,80	2,00	2,50	2,50	2,00
1	DNC-Chain Layer-1 có cấp phép	Ngoài NS	15,00	15,00	-	-	-	-
2	Mô đun 1	Ngoài NS	8,80	8,80	-	-	-	-

Mã	Tên hạng mục	Nguồn vốn	Tổng	2026	2027	2028	2029	2030
3	Mô đun 2	NSDP	5,00	5,00	-	-	-	-
4	Mô đun 3	NSDP	3,00	3,00	-	-	-	-
5	Mô đun 4	NSDP	6,00	6,00	-	-	-	-
6	Mô đun 5	NSDP	3,00	3,00	-	-	-	-
7	Mô đun 6	NSDP	6,00	6,00	-	-	-	-
8	Mô đun 7	NSDP	4,00	4,00	-	-	-	-
9	Kết nối DNC-Chain với LGSP	NSDP	2,00	2,00	-	-	-	-
10	Giám sát, vận hành, dự phòng, ứng cứu sự cố	NSDP	10,00	1,00	2,00	2,50	2,50	2,00
III	TRIỂN KHAI 10 SẢN PHẨM	Hỗn hợp	151,40	25,80	25,50	34,90	33,50	31,70
SP1	Tổng SP1	NSDP	18,70	6,50	4,80	3,10	2,10	2,20
1	- Phát triển ứng dụng và tích hợp CSDL	NSDP	10,00	6,00	3,00	1,00	-	-
2	- Vận hành (cloud, bảo trì, nâng cấp)	NSDP	8,70	0,50	1,80	2,10	2,10	2,20
SP2	Tổng SP2	NSDP	15,70	5,90	4,50	1,80	1,80	1,70

Mã	Tên hạng mục	Nguồn vốn	Tổng	2026	2027	2028	2029	2030
1	- Phát triển ứng dụng	NSĐP	6,00	4,00	2,00	-	-	-
2	- Tích hợp blockchain	NSĐP	2,50	1,50	1,00	-	-	-
3	- Vận hành	NSĐP	7,20	0,40	1,50	1,80	1,80	1,70
SP3	Tổng SP3	NSĐP	7,44	0,80	1,00	2,00	1,90	1,74
1	- Phát triển ứng dụng	NSĐP	3,00	0,50	0,70	1,00	0,50	0,30
2	- Tích hợp blockchain	NSĐP	1,50	0,30	0,30	0,50	0,20	0,20
3	- Vận hành	NSĐP	2,94	-	-	0,50	1,20	1,24
SP4	Tổng SP4	NSĐP	15,70	1,50	2,20	4,00	4,00	4,00
1	- Phát triển ứng dụng	NSĐP	6,00	1,00	1,50	2,00	1,00	0,50
2	- Tích hợp blockchain	NSĐP	2,50	0,50	0,70	0,80	0,30	0,20
3	- Vận hành	NSĐP	7,20	-	-	1,20	2,70	3,30
SP5	Tổng SP5	NSĐP	7,44	0,80	1,00	2,00	1,90	1,74

Mã	Tên hạng mục	Nguồn vốn	Tổng	2026	2027	2028	2029	2030
1	- Phát triển ứng dụng	NSDP	3,00	0,50	0,70	1,00	0,50	0,30
2	- Tích hợp blockchain	NSDP	1,50	0,30	0,30	0,50	0,20	0,20
3	- Vận hành	NSDP	2,94	-	-	0,50	1,20	1,24
SP6	Tổng SP6	Hỗn hợp	21,50	2,00	2,50	6,00	5,50	5,50
1	- Phần quản lý nhà nước, tích hợp, giám sát	NSDP	10,75	1,00	1,25	3,00	2,75	2,75
2	- Phần vận hành thương mại	Ngoài NS	10,75	1,00	1,25	3,00	2,75	2,75
SP7	Tổng SP7	Hỗn hợp	18,76	2,00	2,50	5,00	4,80	4,46
1	- Phần quản lý nhà nước, tích hợp, giám sát	NSDP	9,38	1,00	1,25	2,50	2,40	2,23
2	- Phần vận hành thương mại	Ngoài NS	9,38	1,00	1,25	2,50	2,40	2,23
SP8	Tổng SP8	Ngoài NS	19,00	4,00	4,00	4,00	4,00	3,00
1	- Nền tảng thương mại (theo cơ chế sandbox đã cấp)	Ngoài NS	12,00	3,00	3,00	2,50	2,00	1,50
2	- Tích hợp lớp giám sát với DNC-Chain	Ngoài NS	2,00	0,50	0,50	0,50	0,50	-
3	- Vận hành và duy trì	Ngoài NS	5,00	0,50	0,50	1,00	1,50	1,50
SP9	Tổng SP9	Ngoài NS	18,00	1,50	2,00	4,50	5,00	5,00
1	- Nền tảng phát hành, giao dịch RWA	Ngoài NS	10,00	1,00	1,20	2,70	2,80	2,30
2	- Hệ thống lưu ký (custody) và tích hợp DNC-Chain	Ngoài NS	3,50	0,50	0,80	1,00	0,70	0,50

Mã	Tên hạng mục	Nguồn vốn	Tổng	2026	2027	2028	2029	2030
3	- Vận hành thương mại	Ngoài NS	4,50	-	-	0,80	1,50	2,20
SP10	Tổng SP10	Hỗn hợp	9,16	0,80	1,00	2,50	2,50	2,36
1	- Quản lý nhà nước, tích hợp, giám sát	NSDP	4,58	0,40	0,50	1,25	1,25	1,18
2	- Phân thương mại theo cơ chế IFC	Ngoài NS	4,58	0,40	0,50	1,25	1,25	1,18
IV	CHUẨN HOÁ DỮ LIỆU, TÍCH HỢP, BẢO ĐẢM AN TOÀN THÔNG TIN VÀ AN NINH MẠNG	NSDP	5,00	1,60	1,10	1,10	0,60	0,60
1	Chuẩn hoá dữ liệu và xác định phạm vi dữ liệu đưa vào sử dụng	NSDP	1,20	0,50	0,30	0,15	0,15	0,10
2	Bảo đảm chất lượng, đối soát và xử lý sai lệch dữ liệu trong tích hợp	NSDP	0,60	0,15	0,15	0,15	0,05	0,10
3	Bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân	NSDP	2,70	0,85	0,55	0,70	0,30	0,30
4	Tổ chức kiểm tra, đánh giá, kiểm soát tuân thủ	NSDP	0,50	0,10	0,10	0,10	0,10	0,10
V	NGUỒN NHÂN LỰC, NĂNG LỰC TRIỂN KHAI VÀ HỆ SINH THÁI	NSDP	38,18	9,10	9,02	7,02	7,02	6,02
1	Đào tạo, bồi dưỡng nguồn nhân lực blockchain (bao gồm đào tạo đội ngũ vận hành, tích hợp, kiểm thử, ATTT; bồi dưỡng quản lý nhà nước, giám sát, quản trị rủi ro, năng lực phối hợp mô hình gắn với IFC)	NSDP	4,00	1,20	1,20	0,60	0,60	0,40

Mã	Tên hạng mục	Nguồn vốn	Tổng	2026	2027	2028	2029	2030
2	Ban hành và tổ chức áp dụng Khung năng lực vận hành hệ thống blockchain thành phố	NSDP	0,180	0,10	0,020	0,020	0,020	0,020
3	Phát triển hệ sinh thái doanh nghiệp, viện nghiên cứu và cơ sở đào tạo	NSDP	6,00	1,50	1,50	1,00	1,00	1,00
4	Ban hành và triển khai Kế hoạch cụ thể hoá cơ chế thành phố là khách hàng đầu tiên theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025	NSDP	10,00	2,00	2,00	2,00	2,00	2,00
5	Ban hành Danh mục định hướng đặt hàng; Kế hoạch phối hợp với Chương trình khoa học, công nghệ và ĐMST quốc gia phát triển sản phẩm, dịch vụ công nghệ chiến lược ưu tiên triển khai ngay theo Quyết định số 2815/QĐ-TTg; tổ chức thực hiện đặt hàng	NSDP	10,00	2,00	2,00	2,00	2,00	2,00
6	Hợp tác quốc tế, chuyển giao công nghệ và thu hút chuyên gia	NSDP	8,00	2,30	2,30	1,40	1,40	0,60
VI	DỰ PHÒNG	NSDP	10,00	2,00	2,00	2,00	2,00	2,00
VII	TỔNG CỘNG	Hỗn hợp	268	92,52	39,72	47,62	45,72	42,42

Ghi chú:

(1) Hợp phần I (Thế chế và khung pháp lý): các nhiệm vụ được triển khai trong kinh phí hoạt động thường xuyên của các cơ quan chủ trì.

(2) Hợp phần V Khoản 2, 4, 5 (Khung năng lực; Kế hoạch khách hàng đầu tiên; Danh mục đặt hàng): các văn bản thể chế được ban hành theo chức năng tham mưu.

(3) **Các sản phẩm Tầng 4 (SP8, SP9, SP10):** thực hiện theo cơ chế riêng; ngân sách thành phố chỉ tham gia ở phần quản lý, giám sát, tích hợp kỹ thuật với DNC-Chain, tuân thủ, quản trị rủi ro và bảo đảm chức năng quản lý nhà nước; phần thương mại do doanh nghiệp đầu tư. Riêng đối với SP9, SP10 (ghi 0,00 tỷ NSĐP), kinh phí quản lý, giám sát, tích hợp kỹ thuật với DNC-Chain và bảo đảm chức năng quản lý nhà nước được phân bổ tập trung trong Hợp phần II thông qua hạng mục "Giám sát, vận hành, dự phòng, ứng cứu sự cố DNC-Chain" (10,00 tỷ NSĐP), không bố trí riêng theo từng sản phẩm Tầng 4 để tránh trùng lặp.

(4) **SP6, SP10:** cơ cấu kinh phí hỗn hợp 50/50 giữa NSĐP và Ngoài NS.

(5) **SP7:** cơ cấu kinh phí hỗn hợp 50/50 giữa NSĐP (phần quản lý nhà nước, tích hợp, giám sát) và Ngoài NS (phần vận hành thương mại).

(6) **Cấu thành ATTT phân bổ giữa các Hợp phần:** phần ATTT cho hạ tầng DNC-Chain được phân bổ trong Hợp phần II thông qua Mô đun 3 (Quản lý khoá và phân quyền) 3,00 tỷ, nhiệm vụ "Giám sát, vận hành, dự phòng, ứng cứu sự cố DNC-Chain" 10,00 tỷ, các yêu cầu ATTT tích hợp trong từng mô đun nền tảng dùng chung; phần ATTT cho dữ liệu nguồn và quá trình tích hợp được phân bổ trong Hợp phần IV (4,50 tỷ). Tổng cấu thành ATTT (gồm khoản chi trực tiếp và gián tiếp tại các hợp phần) đạt khoảng 5,7-6,5% tổng nhu cầu kinh phí Đề án.

(7) **Cấu thành nguồn nhân lực blockchain:** kinh phí Hợp phần V Khoản 1 (4,00 tỷ đồng cho đào tạo, bồi dưỡng) được bố trí cho đội ngũ vận hành, tích hợp, kiểm thử, ATTT của thành phố và bồi dưỡng cán bộ quản lý nhà nước, giám sát, quản trị rủi ro, phối hợp mô hình Tầng 4. Chỉ tiêu ≥ 1.000 nhân lực blockchain có kiến thức và kỹ năng trên địa bàn đến năm 2030 (Chỉ tiêu 18 Bảng 11 Chương VI) được bảo đảm thông qua kết hợp 04 nguồn: (i) đào tạo, bồi dưỡng từ ngân sách thành phố theo Hợp phần V Khoản 1; (ii) chương trình đào tạo của các cơ sở giáo dục đại học, cao đẳng trên địa bàn theo Hợp phần V Khoản 3 (6,00 tỷ); (iii) hợp tác quốc tế, chuyển giao công nghệ và thu hút chuyên gia theo Hợp phần V Khoản 6 (8,00 tỷ); (iv) doanh nghiệp tự đào tạo nhân lực phục vụ hoạt động trên hệ sinh thái blockchain.

Phụ lục III

DANH MỤC NHIỆM VỤ, CHƯƠNG TRÌNH, DỰ ÁN, SẢN PHẨM, HẠNG MỤC ĐẦU TƯ VÀ ĐẦU MỐI CHỦ TRÌ

Phụ lục III tổ chức danh mục các nhiệm vụ, hạng mục và sản phẩm của Đề án theo 06 hợp phần, bám sát 05 nhóm nhiệm vụ và giải pháp tại Chương IV và trục phân tầng 04 cấp độ sản phẩm tại Chương III; cơ cấu kinh phí chi tiết theo từng năm được quy định tại Phụ lục II kèm theo Đề án.

Đơn vị tính kinh phí: tỷ đồng.

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
I	THẺ CHẾ VÀ KHUNG PHÁP LÝ					2026-2030	0,62	0,62	0,00
1	Rà soát, hệ thống hóa văn bản pháp lý	Khung chung	Sở Khoa học và Công nghệ	Sở Tư pháp; các sở, ngành liên quan	Báo cáo rà soát; danh mục văn bản của thành phố cần ban hành	2026-2030	0,10	0,10	0,00
2	Quy chế quản trị, vận hành và khai thác DNC-Chain; Quy chế tiếp nhận, thẩm định, phê duyệt, triển khai và quản lý vòng đời ứng dụng	Khung chung	Sở Khoa học và Công nghệ	Công an thành phố; VP UBND TP; Sở Tư pháp; các sở, ngành liên quan	Quy chế phiên bản 1.0 (2026); phiên bản chính thức (2027); rà soát, cập nhật định kỳ	2026-2030	0,130	0,130	0,00
3	Bộ tiêu chuẩn kỹ thuật và yêu cầu kết nối, chia sẻ, kiểm chứng dữ liệu trên DNC-Chain	Khung chung	Sở Khoa học và Công nghệ	Công an thành phố; các sở, ngành có hệ thống nguồn; đơn vị thuộc Bộ Khoa học và Công nghệ	Phiên bản tối thiểu (2026); phiên bản đầy đủ (2027); rà soát, cập nhật định kỳ	2026-2030	0,130	0,130	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
4	Quy chế phối hợp liên ngành và quy trình xử lý vướng mắc trong triển khai Đề án	Khung chung	Sở Khoa học và Công nghệ	Văn phòng UBND thành phố; các sở, ngành; UBND phường, xã	Quy chế phối hợp liên ngành; quy trình xử lý vướng mắc	2026-2030	0,130	0,130	0,00
5	Quy chế bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân đối với DNC-Chain và các ứng dụng kết nối	Khung chung	Sở Khoa học và Công nghệ	Công an thành phố; Sở Tư pháp; cơ quan, đơn vị liên quan	Quy chế ATTT, ANM, BVDLCN; cơ chế kiểm tra, ứng cứu sự cố	2026-2030	0,130	0,130	0,00
II	HẠ TẦNG BLOCKCHAIN DÙNG CHUNG (DNC-CHAIN)					2026-2030	62,80	39,00	23,80
1	DNC-Chain Layer-1 có cấp phép	Hạ tầng	Sở Khoa học và Công nghệ	Trung tâm dữ liệu thành phố; doanh nghiệp	Hạ tầng Layer-1 vận hành ổn định	2026-2027	15,00	0,00	15,00
2	Mô đun 1 (Cầu nối Đa chuỗi)	Hạ tầng	Sở Khoa học và Công nghệ	Cơ quan, đơn vị liên quan; đơn vị kỹ thuật	Mô đun dùng chung được triển khai	2026-2027	8,80	0,00	8,80
3	Mô đun 2 (Tích hợp, tạo bằng chứng xác minh và đối soát hồ sơ điện tử)	Hạ tầng	Sở Khoa học và Công nghệ	VP UBND thành phố; cơ quan, đơn vị liên quan; đơn vị kỹ thuật	Mô đun dùng chung được triển khai	2026-2027	5,00	5,00	0,00
4	Mô đun 3 (Quản lý khoá và phân quyền)	Hạ tầng	Sở Khoa học và Công nghệ	Công an thành phố; cơ quan, đơn vị liên quan; đơn vị kỹ thuật	Mô đun dùng chung được triển khai	2026-2027	3,00	3,00	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
5	Mô đun 4 (Quản lý giao dịch và Token)	Hạ tầng	Sở Khoa học và Công nghệ	Cơ quan, đơn vị liên quan; đơn vị kỹ thuật	Mô đun dùng chung được triển khai	2026-2027	6,00	6,00	0,00
6	Mô đun 5 (Quản lý smart contract)	Hạ tầng	Sở Khoa học và Công nghệ	Cơ quan, đơn vị liên quan; đơn vị kỹ thuật	Mô đun dùng chung được triển khai	2026-2027	3,00	3,00	0,00
7	Mô đun 6 (Quản lý ứng dụng và marketplace)	Hạ tầng	Sở Khoa học và Công nghệ	Cơ quan, đơn vị liên quan; đơn vị kỹ thuật	Mô đun dùng chung được triển khai	2026-2027	6,00	6,00	0,00
8	Mô đun 7 (Hub làm sạch dữ liệu)	Hạ tầng	Sở Khoa học và Công nghệ	Công an thành phố; Sở Tư pháp; cơ quan, đơn vị liên quan	Mô đun dùng chung được triển khai	2026-2027	4,00	4,00	0,00
9	Kết nối DNC-Chain với LGSP	Hạ tầng	Sở Khoa học và Công nghệ	Trung tâm dữ liệu thành phố; cơ quan, đơn vị liên quan	Tích hợp DNC-Chain với LGSP	2026-2027	2,00	2,00	0,00
10	Giám sát, vận hành, dự phòng, ứng cứu sự cố DNC-Chain	Hạ tầng	Sở Khoa học và Công nghệ	Trung tâm dữ liệu thành phố; Công an thành phố; cơ quan, đơn vị liên quan	Hệ thống giám sát, sao lưu, phục hồi vận hành ổn định	2026-2030	10,00	10,00	0,00
III	TRIỂN KHAI 10 SẢN PHẨM THEO 04 TẦNG CẤP ĐỘ					2026-2030	151,40	89,69	61,71
1	SP1 - Hệ thống bảo đảm toàn vẹn hồ sơ điện tử trên blockchain	1	Sở Khoa học và Công nghệ; các sở, ban, ngành có hệ thống	VP UBND thành phố; các sở, ban, ngành có hệ thống nguồn; doanh nghiệp công nghệ	Sản phẩm đưa vào vận hành	2026-2027	18,70	18,70	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
			nguồn						
2	SP2 - Hệ thống xác minh văn bằng, chứng chỉ trên blockchain	1	Sở Giáo dục và Đào tạo	Đại học Đà Nẵng; các cơ sở giáo dục; Sở Khoa học và Công nghệ; doanh nghiệp công nghệ	Sản phẩm đưa vào vận hành	2026-2027	15,70	15,70	0,00
3	SP3 - Bản sao số đô thị (Digital Twin) tích hợp blockchain	2	Sở Khoa học và Công nghệ; Sở Xây dựng; Sở Nông nghiệp và Môi trường	UBND phường, xã; đơn vị quản lý hạ tầng đô thị; doanh nghiệp	Sản phẩm đưa vào vận hành năm 2029	2026-2030	7,44	7,44	0,00
4	SP4 - Hệ thống xác minh hồ sơ y tế trên blockchain	2	Sở Y tế	Các bệnh viện, cơ sở khám chữa bệnh; Sở Khoa học và Công nghệ; Công an thành phố; doanh nghiệp công nghệ	Sản phẩm đưa vào vận hành năm 2029	2026-2030	15,70	15,70	0,00
5	SP5 - Sàn giao dịch dữ liệu thành phố tích hợp blockchain	3	Sở Khoa học và Công nghệ; các cơ quan, đơn vị chủ quản dữ	VP UBND thành phố; Trung tâm dữ liệu thành phố; Công an thành phố; doanh nghiệp công	Sản phẩm đưa vào vận hành năm 2029	2026-2030	7,44	7,44	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
			liệu được phép chia sẻ	nghệ					
6	SP6 - Sàn giao dịch tài sản sở hữu trí tuệ tích hợp blockchain	3	Sở Khoa học và Công nghệ; các chủ sở hữu tài sản sở hữu trí tuệ	Cục Sở hữu trí tuệ; Sở Tài chính; các trung tâm đổi mới sáng tạo; doanh nghiệp	Sản phẩm đưa vào vận hành năm 2029	2026-2030	21,50	10,75	10,75
7	SP7 - Chương trình khách hàng trung thành của thành phố (City Loyalty Program) tích hợp blockchain	3	Sở Văn hoá, Thể thao và Du lịch	Sở Công Thương; Sở Khoa học và Công nghệ; doanh nghiệp du lịch, thương mại, dịch vụ	Sản phẩm đưa vào vận hành năm 2029	2026-2030	18,76	9,38	9,38
8	SP8 - Nền tảng chuyển đổi TSMH sang tiền pháp định (sandbox)	4	Sở Khoa học và Công nghệ; Cơ quan điều hành IFC tại Đà Nẵng	Sở Tài chính; Ngân hàng Nhà nước khu vực 9; Công an thành phố	Tiếp tục theo cơ chế sandbox; tích hợp DNC-Chain	Theo cơ chế sandbox đã được cấp phép	19,00	0,00	19,00
9	SP9 - Nền tảng phát hành, lưu ký và giao dịch tài sản mã hoá (RWA)	4	Cơ quan điều hành IFC tại Đà Nẵng	Sở Tài chính; Ngân hàng Nhà nước khu vực 9; Sở Tư pháp; Công an thành phố; doanh nghiệp công nghệ tài chính	Triển khai theo cơ chế riêng gắn với Cơ quan điều hành IFC tại Đà Nẵng; tích hợp DNC-Chain	Theo cơ chế riêng	18,00	0,00	18,00
10	SP10 - Nền tảng gọi	4	Cơ quan điều	Sở Tài chính; các	Triển khai	Theo cơ	9,16	4,58	4,58

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
	vốn cộng đồng trên blockchain		hành IFC tại Đà Nẵng	trung tâm đổi mới sáng tạo; Ngân hàng Nhà nước khu vực 9; doanh nghiệp	theo cơ chế riêng gắn với Cơ quan điều hành IFC tại Đà Nẵng; tích hợp DNC-Chain	chế riêng			
IV	CHUẨN HOÁ DỮ LIỆU, TÍCH HỢP, BẢO ĐẢM AN TOÀN THÔNG TIN VÀ AN NINH MẠNG					2026-2030	5,00	5,00	0,00
1	Chuẩn hoá dữ liệu và xác định phạm vi dữ liệu đưa vào sử dụng trên DNC-Chain	Khung chung	Các sở, ban, ngành chủ trì dữ liệu nguồn	Sở Khoa học và Công nghệ	Dữ liệu nguồn các ngành được chuẩn hoá; danh mục dữ liệu đưa vào sử dụng theo từng SP	2026-2030	1,20	1,20	0,00
2	Bảo đảm chất lượng, đối soát và xử lý sai lệch dữ liệu trong tích hợp	Khung chung	Các sở, ban, ngành chủ trì dữ liệu nguồn	Sở Khoa học và Công nghệ	Kết quả đối soát dữ liệu định kỳ; sai lệch được phát hiện và xử lý; mức độ tin cậy dữ liệu đạt yêu cầu vận hành	2026-2030	0,60	0,60	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
3	Bảo đảm an toàn thông tin, an ninh mạng và bảo vệ dữ liệu cá nhân	Khung chung	Các sở, ban, ngành chủ trì dữ liệu nguồn	Sở Khoa học và Công nghệ; Công an thành phố; Trung tâm dữ liệu thành phố	Hệ thống giám sát ATTT vận hành; sự cố được phát hiện, cảnh báo, xử lý kịp thời; dữ liệu cá nhân được bảo vệ theo quy định	2026-2030	2,70	2,70	0,00
4	Tổ chức kiểm tra, đánh giá, kiểm soát tuân thủ trong quá trình vận hành	Khung chung	Sở Khoa học và Công nghệ	Công an thành phố; Cơ quan, đơn vị liên quan; đơn vị kiểm toán độc lập	Kết quả kiểm định mật mã; kết quả kiểm toán bảo mật hợp đồng thông minh định kỳ; báo cáo đánh giá tác động dữ liệu cá nhân; kết quả rà soát tuân thủ pháp lý	2026-2030	0,50	0,50	0,00
V	NGUỒN NHÂN LỰC, NĂNG LỰC TRIỂN KHAI VÀ HỆ SINH THÁI					2026-2030	38,18	38,18	0,00
1	Đào tạo, bồi dưỡng nguồn nhân lực blockchain (đào tạo đội ngũ vận hành, tích hợp, kiểm thử, an	Khung chung	Sở Khoa học và Công nghệ; Công an thành phố; Sở Tài chính;	Sở Nội vụ; Đại học Đà Nẵng; các cơ sở đào tạo, viện nghiên cứu	Đội ngũ nhân lực blockchain được đào tạo, bồi dưỡng theo vai trò;	2026-2030	4,00	4,00	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
	toàn thông tin; bồi dưỡng quản lý nhà nước, giám sát, quản trị rủi ro; bồi dưỡng năng lực phối hợp mô hình Tầng 4)		IFC Đà Nẵng; Cơ quan, đơn vị chủ trì sản phẩm		chương trình đào tạo tại cơ sở đào tạo đại học				
2	Ban hành và tổ chức áp dụng Khung năng lực vận hành hệ thống blockchain thành phố	Khung chung	Sở Khoa học và Công nghệ	Sở Nội vụ; các cơ sở đào tạo; Công an thành phố	Khung năng lực theo vai trò được ban hành; áp dụng trong tuyển dụng, bố trí, đánh giá cán bộ	2026-2030	0,18	0,18	0,00
3	Phát triển hệ sinh thái doanh nghiệp, viện nghiên cứu và cơ sở đào tạo	Khung chung	Sở Khoa học và Công nghệ;	Sở Tài chính; Ban Xúc tiến và Hỗ trợ đầu tư thành phố; Hiệp hội Blockchain và Tài sản số Việt Nam (VBA); các trung tâm đổi mới sáng tạo; doanh nghiệp; viện nghiên cứu	Ít nhất 30 doanh nghiệp tham gia hệ sinh thái blockchain (đến 2030)	2026-2030	6,00	6,00	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
4	Ban hành và triển khai Kế hoạch cụ thể hoá cơ chế thành phố là khách hàng đầu tiên đối với sản phẩm blockchain theo Quyết định số 2815/QĐ-TTg ngày 28/12/2025	Khung chung	Sở Khoa học và Công nghệ	Sở Tài chính; các sở, ngành có nhu cầu mua sắm; doanh nghiệp	Kế hoạch được ban hành; ít nhất 08 sản phẩm blockchain được thành phố tiếp nhận theo cơ chế khách hàng đầu tiên	2026-2030	10,00	10,00	0,00
5	Ban hành Danh mục đặt hàng nhiệm vụ nghiên cứu; Kế hoạch phối hợp với Chương trình khoa học, công nghệ và ĐMST quốc gia phát triển sản phẩm, dịch vụ công nghệ chiến lược ưu tiên triển khai ngay	Khung chung	Sở Khoa học và Công nghệ	Sở Tài chính; Bộ Khoa học và Công nghệ; viện nghiên cứu; cơ sở đào tạo; doanh nghiệp	Danh mục đặt hàng được ban hành; ít nhất 08 nhiệm vụ đặt hàng được triển khai; tham gia Chương trình quốc gia	2026-2030	10,00	10,00	0,00
6	Hợp tác quốc tế, chuyển giao công nghệ và thu hút chuyên gia blockchain	Khung chung	Sở Khoa học và Công nghệ; Ban Hỗ trợ và Xúc tiến đầu tư thành phố	Sở Ngoại vụ; các cơ sở đào tạo; đối tác quốc tế	Ít nhất 05 thỏa thuận, chương trình hợp tác quốc tế; chuyên gia quốc tế tham gia đào tạo và chuyển giao công nghệ	2026-2030	8,00	8,00	0,00

Mã	Tên nhiệm vụ/hạng mục	Tầng	Cơ quan chủ trì	Cơ quan phối hợp	Kết quả đầu ra	Thời gian	Tổng	NSDP	Ngoài NS
VI	DỰ PHÒNG					2026-2030	10,00	10,00	0,00
VII	TỔNG CỘNG					2026-2030	268	182,49	85,51

Ghi chú:

(1) **Cơ quan chủ trì:** đối với các sản phẩm ứng dụng (HP III), nếu cơ quan chủ trì sản phẩm và cơ quan chủ trì dữ liệu nguồn khác nhau, cơ quan chủ trì dữ liệu nguồn được ghi bằng chữ nghiêng với chú thích "(chủ trì dữ liệu nguồn)". Trường hợp hai đầu mối là cùng một cơ quan, chỉ ghi tên cơ quan đó một lần.

(2) **Hợp phần I (Thể chế và khung pháp lý):** các nhiệm vụ được triển khai trong kinh phí hoạt động thường xuyên của các cơ quan chủ trì; không bố trí kinh phí riêng tại Phụ lục II, III.

(3) **Hợp phần V Khoản 2, 4, 5 (Khung năng lực; Kế hoạch khách hàng đầu tiên; Danh mục đặt hàng):** các văn bản thể chế được ban hành theo chức năng tham mưu, không bố trí kinh phí riêng.

(4) **Các sản phẩm Tầng 4 (SP8, SP9, SP10):** thực hiện theo cơ chế riêng; ngân sách nhà nước chỉ tham gia ở phần quản lý, giám sát, tích hợp kỹ thuật với DNC-Chain, tuân thủ, quản trị rủi ro và bảo đảm chức năng quản lý nhà nước; phần thương mại do doanh nghiệp đầu tư.

(5) **SP6, SP10:** cơ cấu kinh phí hỗn hợp 50/50 giữa NSDP và Ngoài NS.

(6) **SP7:** cơ cấu kinh phí hỗn hợp 50/50 giữa NSDP (phần quản lý nhà nước, tích hợp, giám sát) và Ngoài NS (phần vận hành thương mại).

(7) **Cấu thành ATTT phân bổ giữa các Hợp phần:** phần ATTT cho hạ tầng DNC-Chain được phân bổ trong Hợp phần II thông qua Mô đun 3 (Quản lý khoá và phân quyền), nhiệm vụ "Giám sát, vận hành, dự phòng, ứng cứu sự cố DNC-Chain" và các yêu cầu ATTT tích hợp trong từng mô đun nền tảng dùng chung; phần ATTT cho dữ liệu nguồn và quá trình tích hợp được phân bổ trong Hợp phần IV. Tổng cấu thành ATTT (gồm khoản chi trực tiếp và gián tiếp tại các hợp phần) đạt khoảng 5,7-6,5% tổng nhu cầu kinh phí Đề án.