18 May 2026

Submitted via MAS electronic consultation portal and email

To: Monetary Authority of Singapore (MAS)

Re: Consultation Paper P009-2026 — Prudential Treatment of Cryptoassets on Permissionless Blockchains

---

Executive Summary

The Avalanche Policy Coalition ("APC") welcomes the opportunity to respond to Consultation Paper P009-2026 on the Prudential Treatment of Cryptoassets on Permissionless Blockchains (the "Consultation"). APC is the policy hub for the Avalanche community, serving as a premier resource on foundational blockchain policy and regulatory issues. Our guiding principles for policymakers and regulators encourage workable laws and rules that are easy to understand and apply. More information is available at https://www.avalanchepolicy.com.

APC was founded by Ava Labs, Inc., a technology company formed in 2018 with the aim of advancing blockchain and related technologies in order to foster greater adoption of this new database layer of the internet. Through the work of Ava Labs and others, the Avalanche Primary Network was launched by a diversified group of validators in September 2020, bringing its novel consensus mechanism to the world. The Avalanche protocol also affords users the ability to build interoperable, custom Layer-1 blockchains ("L1s") that can integrate compliance requirements with bespoke programming for virtually any use case. Resources related to the Avalanche technology are available at https://build.avax.network. The Exhibit to this letter lists numerous examples of custom L1s built with the Avalanche technology and different assets, items and things that have been tokenized on Avalanche.

We appreciate the opportunity to respond to the Consultation and applaud MAS's proposals to adopt a principle-based, risk-sensitive framework that assesses cryptoassets by what they actually are. This concept is consistent with APC's longstanding token classification methodology, which is based on the nature of the asset. MAS also places the requirements where they properly belong, on the intermediary layer, not infrastructure providers. We understand MAS to be applying common principles of bank risk management to cryptoassets when making determinations about their categorization for capital treatment. We applaud that thinking.

In this letter, we first discuss our principles of token classification and the distinction between intermediaries and infrastructure providers, and explain how MAS's framework reflects those ideas. Next, we turn to a description of the Avalanche network and how Avalanche L1s are designed to satisfy the principle-based requirements and deeming provisions proposed in the Consultation. We then summarise certain Avalanche implementations under MAS-supervised initiatives. Finally, we address each of the four consultation questions with specific observations and recommendations tied to the previous sections. We conclude with a summary of our recommendations.

1. Token Classification and the Infrastructure/Intermediary Distinction

Two of our continuing policy priorities are directly relevant to this Consultation. We set them out here as a foundation for the submission.

Token Classification Based on the Nature of the Asset

APC advocates for a token classification system grounded in the nature of the asset, item or bundle of rights a token represents, not the technology used to record it. The core principle is simply illustrated: a tokenised bond is a bond; a tokenised money market fund share is a fund share; a tokenised event ticket is a ticket to an event. Blockchain technology changes the means of representation, not the substance of what is being represented or its legal nature. Treating all tokens the same because they are recorded on a blockchain makes no more sense than treating a concert ticket, a share certificate, and a property deed the same because they are all printed on paper.

This principle is directly reflected in MAS's classification condition 1, which asks whether a cryptoasset is a tokenised traditional financial instrument or an asset with an effective stabilisation mechanism: In other words, what the asset actually is, based on its features and functions. APC applauds this approach as the best starting point for any prudential classification framework, because it produces rules that are legally accurate, technology-neutral, easy to apply, and proportionate to actual risk.

The Exhibit to this letter illustrates the breadth of assets that have been tokenised on Avalanche, spanning government money market funds, private credit, real estate, insurance, commodities, payment instruments, and consumer loyalty programmes. Each of these asset types has its own established legal and regulatory characterisation that should follow the asset onto the blockchain. We applaud MAS for adopting this approach in the Consultation.

Infrastructure vs. Intermediary: Regulating the Right Layer

The second longstanding APC policy principle is the distinction between intermediary functions and infrastructure. Blockchain infrastructure, including validators, node operators, software developers, and hardware and communications providers, provides the common infrastructure rails for all blockchain use cases, including those that constitute regulated activities. It is the specific businesses that use those rails, such as banks, issuers, custodians, and payment providers, that should bear regulatory obligations. Pushing regulatory requirements to the infrastructure layer would be the equivalent of requiring internet service providers and browser software providers to be regulated as financial intermediaries simply because financial transactions occur over the internet by people using browsers.

This distinction is reflected in MAS's approach in this Consultation. The principle-based requirements and deeming provisions in Annexes C and D are directed at banks, rather than the underlying blockchain infrastructure providers. This is the correct approach: it places obligations where they belong, on the institutions that underwrite, take positions in, and issue cryptoassets, while preserving the neutrality of the infrastructure layer.

2. About the Avalanche Network

The Avalanche Primary Network

The Avalanche Primary Network is a public, permissionless blockchain network secured by a distributed set of independently operated validators located around the globe. Any party meeting the minimum staking requirement can become a validator. Validator influence is weighted by stake amount, creating strong economic incentives for honest behaviour.

The Primary Network includes an implementation of the Ethereum Virtual Machine (EVM), supporting smart contract programming and is backward-compatible with Ethereum developer tooling. It is also where coordination of validators across all Avalanche L1s happens to enable interoperability among all L1s that choose it.

Because of the EVM implementation, any smart contract that has been deployed on Ethereum can be deployed on the Avalanche, with the benefit of Avalanche's faster finality and lower transaction costs. Developers can also write smart contracts in Solidity specifically for Avalanche and interact with them using standard Ethereum tooling. This includes smart contracts that implement compliance functions: for example, a token contract can be programmed to enforce transfer restrictions, maintain whitelists of approved holders, implement an AML/CFT program, and freeze or block transactions, all enforced at the smart contract level and auditable on the public blockchain.

Avalanche consensus has several properties that are directly relevant to the prudential requirements in the Consultation. It achieves finality quickly, usually in about 1 second. It is leaderless: any node can propose a transaction, and any node that has staked AVAX can participate in validation. It scales efficiently: the protocol does not degrade as validator participation grows. It is designed to resist sybil attacks, DDoS attacks, and collusion attacks through its adaptive security design. More information can be found at https://build.avax.network/docs/primary-network.

Avalanche L1s

The Avalanche L1 architecture enables any party to deploy a sovereign Layer-1 blockchain with its own validator set, consensus rules, virtual machine, and compliance configuration. Avalanche L1s are not Layer-2 solutions and are not dependent on the Primary Network for their security or finality: each L1 is validated by its own dedicated validator set and achieves consensus independently. L1s may be permissioned or permissionless, may use the Avalanche consensus protocol or another selected consensus mechanism, and may support EVM-compatible or other virtual machines, including custom-developed ones. This means that Avalanche L1s can be configured with native compliance features relevant to Annex C and Annex D. These are documented, production-tested features of the Avalanche L1 framework, demonstrated in the MAS-supervised initiatives described in Section 3 below.

3. Avalanche and MAS-Supervised Initiatives

Please note that the Avalanche network has a direct, multi-year track record of participation in MAS-supervised initiatives. MAS therefore has supervisory experience

with Avalanche's technical and compliance properties in production-adjacent, regulated environments. We summarise the three key engagements below.

Project Guardian — Onyx by J.P. Morgan and Apollo Global (2023)

In November 2023, Onyx by J.P. Morgan and Apollo Global announced a proof-of-concept under MAS's Project Guardian built on an Avalanche Evergreen custom L1, with WisdomTree Asset Management as a further participant. The proof-of-concept demonstrated how tokenised alternative assets, private equity, private credit, real estate, and infrastructure, could be managed through smart contract-driven operations in institutionally compliant portfolios. The Avalanche L1 provided network privacy, permissioning at the validation and transaction levels, and performance isolation from the broader Avalanche ecosystem.

Project Guardian — FX Trades on Evergreen by Citi, T. Rowe Price, Fidelity International (2023)

Ava Labs' managed custom blockchain service was used by several regulated financial institutions to test an innovative application under MAS's Project Guardian: leveraging blockchain infrastructure to price and execute simulated bilateral spot foreign-exchange trades on an Avalanche L1.

Project Orchid — Alipay+ and Grab Cross-Border Payments (2023)

StraitsX, a MAS-licensed Major Payment Institution and issuer of the XSGD stablecoin, deployed an Avalanche L1 to power cross-border payments between Alipay+ users and GrabPay merchants in Singapore under MAS Project Orchid's Purpose Bound Money framework. Avalanche was selected because of its approach to privacy controls and cybersecurity risk management.

MAS BLOOM / Project Orchid — KBank of Thailand Cross-Border Settlement (2024)

Building on the Alipay+/Grab deployment, KBank (Kasikornbank) partnered with StraitsX and Orbix Technology in 2024 to launch a Thailand–Singapore cross-border payment corridor on the same Avalanche L1, under the MAS BLOOM initiative. The partners chose an Avalanche L1 because "regulated digital money benefits from predictable and controlled execution environments," a conclusion reached through direct operational experience under MAS supervision.

These four engagements demonstrate that Avalanche is infrastructure that MAS-licensed and MAS-supervised participants have chosen.

4. Responses to Consultation Questions

Question 1: Overall Principle-Based Approach

APC supports MAS's proposal to replace the existing approach that automatically excludes cryptoassets on permissionless networks from Group 1 with principle-based requirements that focus on the nature of the asset and whether relevant risks have been adequately mitigated. The new approach is consistent with APC's principle that regulation should be based on the nature of the asset and the actual risks it presents, not solely on the technology used to represent it. We understand that this new

methodology would in essence apply normal bank risk management concepts to capital treatment of cryptoassets, not create a completely new paradigm in how banks or assets are regulated.

The prior approach, which treated all assets represented on permissionless blockchain infrastructure as inherently high-risk regardless of actual properties, was not technology-neutral and produced outcomes disproportionate to the real risk profile of well-designed networks. More importantly, it failed to account for the legal classification and characteristics of the assets themselves. Upon adoption of the new rules, a tokenised government bond issued on a permissionless blockchain can properly be categorised based on the same credit and market risk as the traditionally-represented asset. A prudential framework that ignores this legal and economic reality and mandates classification based only on the underlying technology is neither risk-sensitive nor consistent with the asset-based approach that underpins MAS's broader regulatory policies.

Using principle-based requirements also recognizes the maturity that many blockchain networks have achieved. For example, the Avalanche network has operated since September 2020 without a successful 51% attack or chain reorganisation. A framework that cannot differentiate that track record from genuinely high-risk infrastructure is not serving its prudential purpose. Moreover, it would bring regulation in line with the approach to other technologies.

APC has two suggestions. First, one aspect of classification condition 3(b) requires that "all transactions and participants are traceable." We submit that for public permissionless networks the relevant test should be whether transactions can be monitored, screened, investigated, and reconciled, not whether every validator and other network participant can be individually identified. Requiring identification of every infrastructure provider would effectively nullify the principle-based approach and be inconsistent with current regulation and practice with respect to other technologies. The identity of infrastructure providers such as communications networks, hardware manufacturers, and the developers of every piece of software are not always known. A requirement to identify everyone would therefore be disproportionate to the actual prudential objectives. APC recommends that MAS confirm this interpretation in the final rules.

Second, APC would suggest that MAS confirm in the final rules that the principle-based requirements and deeming provisions apply at the level of the specific cryptoasset and its underlying blockchain, not at the level of blockchain technology generally. Avalanche L1s are sovereign Layer-1 networks with their own validator sets and compliance configurations, and should be assessed by reference to their own properties rather than by reference to the Avalanche Primary Network. We develop this point further in our response to Question 2 below.

Question 2: Adequacy of Principle-Based Requirements and Deeming Provisions

APC supports the structure of the principle-based requirements in Annex C and the deeming provisions in Annex D as broadly sufficient and appropriate to mitigate the risks arising from permissionless blockchains, subject to the observations below. APC believes that banks should be allowed to develop their own frameworks for integrating public blockchain technologies into their activities. In that connection, APC has participated in

the development of the Risk Mitigation Framework, a project led by Global Blockchain Business Council and Oliver Wyman to provide a practical resource for banks and others to assess public blockchain technology for use in their activities, including tokenisation of assets (available at https://www.gbbc.io/news/rmf-phase2). This project and others like it show that MAS's proposals are well-founded and practical.

We offer the following observations on the requirements and deeming provisions, and then show how Avalanche can be used to meet them.

Finality. The deeming provisions require a "point of finality" to be defined and documented, at which transaction reversal would be economically or technically impractical. APC supports this formulation. We note that finality is not a single concept in either blockchain or traditional financial infrastructure: different systems achieve it through different mechanisms and on different timescales, and finality is not generally defined in financial regulation, even for traditional settlement systems. In traditional markets, what constitutes finality is typically a matter of common practice, contractual arrangement, or central counterparty rules. Any of these formulations should be acceptable for purposes of the deeming provisions.

Regulators in many jurisdictions have deliberately avoided prescribing a single technical definition of finality for blockchain systems, and APC recommends that MAS do the same. The important prudential question is whether, for the specific cryptoasset and blockchain in question, there is a defined and documented threshold beyond which transactions are effectively irreversible. Banks are well placed to make this assessment, which is consistent with the self-assessment model MAS has proposed. APC recommends that MAS confirm these concepts in the final rules.

Validator set integrity. The deeming provisions address governance risk by requiring either a significantly large number of validator nodes or no single entity controlling a significant share of validator nodes or voting power, together with monitoring, penalisation, and dispute resolution mechanisms. The Consultation rightly recognizes that different networks handle these questions in different ways.

Issuer Controls for AML/CFT and Business Continuity Planning. APC notes that MAS's proposals with respect to these areas might result in indirect regulation of issuers' use of technology. We recommend that MAS give careful consideration to this possible result and that the final rules make clear that MAS is not seeking to have banks impose requirements on issuers and that the Consultation is not designed for MAS to regulate issuer actions. Rather, the final regulations are simply about how banks evaluate the assets they hold and their capital treatment.

How Banks and Issuers Can Deploy on Avalanche. At a high level, we believe that banks and issuers can utilize Avalanche technology for asset issuance in a way that complies with the proposed requirements and deeming provisions. For the Avalanche Primary Network, we set out below a table showing the relevant factors and how Avalanche can be used to meet the requirements.

For Avalanche L1s, they are entirely configurable: an L1 operator can require validators to be regulated entities, to pass KYC/AML checks, to hold specific licences, or to be located in specific jurisdictions, providing an additional layer of compliance assurance beyond what the Primary Network already offers. Accordingly, assets issued on an Avalanche L1 can be programmed to independently meet the requirements. Avalanche

L1s are sovereign Layer-1 networks, not Layer-2 solutions. Each L1 has its own validator set and is not dependent on the Primary Network for its security or finality.

This matters because the principle-based requirements and deeming provisions need to be applied at the correct level of analysis: for assets issued on an Avalanche L1, the relevant blockchain for assessment is the L1 itself, not the Primary Network. The compliance features available for Avalanche L1s, including allow-list precompiles, validator KYC requirements, and data privacy configurations, are the features that are relevant to the deeming provision assessment for those assets.

Turning back to the Avalanche Primary Network, it is secured by hundreds of independently operated validators located around the globe, with stake-weighted influence that prevents any single entity from exercising disproportionate control. The network has monitoring mechanisms to assess validator performance, governance mechanisms to detect and respond to malicious behaviour, and a publicly documented governance framework. Comprehensive statistics on validator counts, stake distribution, and network health are publicly available at https://build.avax.network/. The table below maps the principle-based requirements to Avalanche technical features:

Proposed Requirement	Avalanche Technical Response
Settlement finality	Snowman Consensus achieves finality converging to irreversibility in approximately one second. A defined point of finality can be documented and disclosed. No chain reorganisations on the Primary Network since September 2020. Custom L1s inherit this property or can define their own finality parameters.
Validator governance integrity	The Primary Network has hundreds of globally distributed validators with stake-weighted influence. Statistics available at stats.avax.network. Custom L1s can additionally require validators to pass KYC/AML checks, hold licences, or be geographically restricted.
Technology and attack resistance	Snowman Consensus is designed to resist sybil, DDoS, and collusion attacks. Performance isolation means disruption on one L1 does not affect others. Smart contracts subject to independent audit.
AML/CFT manageability	C-Chain smart contracts can enforce transfer restrictions, whitelists, and AML/CFT screening logic. Custom L1 allow-list precompile contracts restrict who may hold and transact in a cryptoasset to pre-screened, verified entities.
Operational resilience / BCP	Off-chain records can serve as the golden source of transactions in the event of blockchain disruption. Performance isolation of custom L1s limits contagion risk.

Question 3: AML/CFT Requirements

APC broadly supports the inclusion of AML/CFT requirements in the principle-based framework. We note that issuers have not traditionally had AML/CFT obligations,

although many issuers conduct these checks as a prudential matter. We understand why MAS wants banks to ensure that AML/CFT controls are in place. We suggest that MAS make clear that the controls can be imposed not just by the issuer but by other parties, including a bank itself, to satisfy the Annex C and/or Annex D requirements. The important thing is that the controls are in place for the assets held by the bank, not who has implemented them.

From a technical standpoint, the Avalanche network offers two complementary mechanisms for satisfying the AML/CFT requirements in Annex C. First, on the Primary Network's C-Chain, smart contracts can be programmed to enforce AML/CFT requirements at the contract level: a token contract can be written to maintain a whitelist of approved holders, reject transfers to or from non-approved addresses, implement screening logic, and support freeze and seizure functions, all enforced automatically by the smart contract code and auditable on the public blockchain.

Second, the flexibility of Avalanche L1s enables cryptoasset issuers to restrict who may hold and transact in a given asset to pre-screened, verified entities or wallets at the network level, satisfying the deeming provision's whitelisting requirement. These controls are implemented on-chain and are transparent and auditable. Where smart contracts are used to implement permissioning controls, they are subject to the independent audit requirement in Annex D, paragraph 3(b).

APC wishes to highlight, however, that whitelisting should be treated as one of several acceptable methods, rather than the exclusive model. Permissioning and whitelisting are appropriate for many institutional tokenised asset use cases, but the principle-based requirements in Annex C are framed in terms of outcomes (ensuring that AML/CFT risks are adequately mitigated) and MAS should confirm that a range of controls can satisfy those outcomes.

Some examples of equivalent approaches that we recommend MAS recognize include regulated issuance and redemption points with full KYC at on- and off-ramps, real-time wallet screening and sanctions screening, transaction monitoring and blockchain analytics provided by regulated compliance service providers, and the ability to freeze or quarantine implicated assets and report to regulators promptly. Again, these can be implemented by the issuer or by another party, so long as they meet the minimum standards. This flexibility is also consistent with the risk-based approach that underpins Singapore's AML/CFT framework more broadly, which understands that distributed ledgers can enhance AML/CFT compliance by providing broader visibility and traceability than traditional technologies.

Question 4: Exposure and Issuance Caps

APC does not support permanent caps once the rules are finalised. If a permissionless cryptoasset satisfies the principle-based requirements and applicable deeming provisions, it should receive Group 1 treatment on the same basis as other Group 1 assets. A permanent cap would add a non-risk-based overlay that treats permissionless blockchain assets differently from economically equivalent traditional assets even after the relevant risks have been mitigated.

Permanent caps could also produce unintended supervisory consequences. Banks would likely manage exposures well below the caps to avoid the risk of sudden reclassification into Group 2 treatment, reducing the ability of regulated institutions to participate in

cryptoasset markets. That outcome could push activity toward non-bank entities outside the prudential perimeter. This concern has been echoed in the joint industry letter to the Basel Committee on Banking Supervision on cryptoasset prudential standards, which noted that fixed caps create structural disincentives for regulated institutions to offer cryptoasset-related services at scale. APC therefore recommends that MAS retain caps only during the interim period and remove them when the final rules are implemented.

5. Conclusion

APC supports Consultation Paper P009-2026 and its proposals on the whole, subject to the refinements discussed above. With its focus on risk management and due diligence by banks, the proposed framework is principled, technology-neutral, and proportionate. We do not interpret it as requiring anything different from banks for cryptoassets than would be required for assets represented in traditional forms. As such, it reflects the kind of asset-based, risk-focused regulatory thinking that APC advocates for as the foundation for workable blockchain and crypto policy, and it correctly places compliance obligations on the banks that participate in cryptoasset markets rather than on the infrastructure layer.

APC respectfully recommends that MAS:

1. Confirm that the principle-based requirements and deeming provisions apply at the level of the specific cryptoasset and blockchain implementation (smart contract, custom L1, Layer 2, etc), rather than favoring particular technologies, such that sovereign Avalanche L1s with their own validator sets and compliance configurations should be assessed by reference to their own properties.
2. Recognise that finality can be achieved in various ways and, for purposes of the final regulations, can be established by common practice or contractual arrangement, among other means, such that there is no prescribed consensus mechanism, mathematical parameter, or legal formulation of finality.
3. Clarify that traceability means the ability to monitor, screen, investigate, and reconcile transactions — not the identification of every validator or network participant.
4. Confirm that the AML/CFT and other technical requirements can be satisfied either by the issuer or by a third party, including a bank, any of which can use service providers that are not themselves regulated.
5. Treat whitelisting as one of several acceptable means of meeting the AML/CFT requirements, thereby allowing equivalent controls, such as regulated issuance and redemption points, KYC at on- and off-ramps, wallet and sanctions screening, transaction monitoring, and blockchain analytics, to satisfy the requirements.
6. Remove exposure and issuance caps when the final rules are implemented, on the basis that the principle-based requirements provide sufficient substantive safeguards, permanent caps are inconsistent with the technology-neutral approach the framework is designed to achieve, and fixed caps risk pushing cryptoasset activity away from regulated institutions and toward entities outside the prudential perimeter.

APC would welcome the opportunity to meet with MAS to discuss these submissions. Please direct any queries to legal@avalabs.org.

Sincerely yours,

Exhibit: Selected Institutional Projects on Avalanche

The following is a representative list of institutional and regulated use cases built on the Avalanche network, illustrating the breadth of asset types that have been tokenised on the platform.

Tokenisation and Finance

- BlackRock (via Securitize) — BlackRock Digital Liquidity Fund (BUIDL), tokenised money market fund on Avalanche
- Franklin Templeton — Tokenised US Government Money Market Fund (Benji Investments) on Avalanche
- Apollo Global Management & Securitize — Tokenised access to private credit fund on Avalanche
- KKR (via Securitize) — Private equity fund tokenisation on Avalanche
- VanEck (via Securitize) — VBILL tokenised money market fund on Avalanche
- Wellington Management (via Libeara) — ULTRA tokenised money market fund
- Galaxy Digital — Tokenised CLO on Avalanche for structured private credit
- Skybridge Capital — $300 million tokenised hedge fund on Avalanche via Tokeny
- ParaFi Capital (via Securitize) — Tokenised venture fund interest on Avalanche
- FIS Global — Digital Liquidity Gateway for on-chain loan securitisation
- Janus Henderson $250M+ CLO RWA deployment on Avalanche
- Securitize - Obtained tokenization licenses(TSS) in EU limited to Avalanche
- SMBC — Compliant Avalanche L1 infrastructure for stablecoin issuance
- Japan Repo Bonds Tokenization : Avalanche named as the only public-blockchain infrastructure partner in Japan's Tokenized JGB / On-Chain Repo Working Group
- Progmat — Japan's largest security token platform on a dedicated Avalanche L1
- Dinari — Compliant Avalanche L1 for tokenised US public securities (dShares)
- Broadridge — On-chain proxy voting and corporate actions for tokenised equities
- Intain — Dedicated Avalanche L1 for structured finance and securitisation
- NHN KCP — Korea’s largest payment processor stablecoin settlement system
- Listed Avalanche(AVAX) ETFs in the US — VanEck, Grayscale and Bitwise

Cross-Border Payments and Digital Money

- StraitsX (MAS-licensed) — XSGD stablecoin; dedicated Avalanche L1 powering MAS Project Orchid (Alipay+/Grab) and MAS BLOOM (KBank Thailand corridor)
- Visa — Visa-powered Avalanche card for global transactions
- Fonbnk — Cross-border payment on-ramps in Sub-Saharan Africa
- Nonco — FX initiative bridging institutional FX liquidity and stablecoin markets

Privacy, Security and Data Integrity

- California DMV — 42 million vehicle titles on Avalanche for fraud prevention
- Deloitte — Smart contract solutions for disaster relief and fraud prevention
- J.P. Morgan Kinexys — Privacy-preserving finance and settlement infrastructure
- Chainlink — Real-time corporate actions data on-chain
- Bergen County, New Jersey — Land records management on Avalanche

MAS-Supervised Pilots

- **Project Guardian (2023)** — Onyx by J.P. Morgan, Apollo Global Management, WisdomTree: tokenised alternative asset portfolio management on Avalanche Evergreen L1
- **Project Guardian (2023)** — Citi, T. Rowe Price, Fidelity International: on-chain FX pricing and simulated trade execution on private permissioned Avalanche Evergreen Subnet
- **MAS Interlinking Networks Whitepaper (2023)** — Ava Labs named as co-author alongside Apollo, J.P. Morgan, Chainlink, Swift, UBS and others; Avalanche featured as one of three reference network implementations
- **Project Orchid (2023~Live)** — StraitsX, Alipay+, Grab: cross-border Purpose Bound Money payments on dedicated Avalanche L1
- **MAS BLOOM (2025)** — StraitsX, KBank Thailand, Orbix: Thailand–Singapore cross-border settlement corridor on dedicated Avalanche L1