

SoK: Stablecoins in the Quantum Era

Panagiotis Chatzigiannis
VISA Research
USA
pchatzig@visa.com

Suvradip Chakraborty
VISA Research
USA
suvchakr@visa.com

Navid Alapati
VISA Research
USA
nalapati@visa.com

Duc V. Le
Circle Research
USA
levduc112@gmail.com

Abstract

Stablecoins support payments, trading, collateral, and cross-chain settlement across the digital-asset ecosystem. They also concentrate value behind issuer, custody, upgrade, oracle, and bridge keys while inheriting the quantum vulnerabilities of host-chain accounts, consensus, rollups, and privacy systems. This paper presents a Systematization of Knowledge (SoK) on post-quantum stablecoins. We develop a stablecoin-specific threat model, map cryptographic dependencies to monetary control surfaces, and classify migration choices along three dimensions: who can authorize a change, where the change must occur, and whether it is hybrid, post-quantum native, or an encapsulation of a classical component. We emphasize an authority–liability gap: the party able to migrate a component is often different from the holders, exchanges, protocols, or issuers that bear the loss if it fails. We review the relevant cryptographic primitives, but distinguish general blockchain failures from their stablecoin-specific effects. We also examine recent blockchain and issuer-controlled interoperability proposals, and relate migration choices to redemption, continuity, and intervention requirements under current stablecoin regulation. Our findings identify open problems in aggregate and threshold authorization, operation-specific security levels and costs, dormant and wrapped supply, private and compliance-enabled transfers, and measurement of quantum-vulnerable stablecoin exposure.

Keywords

stablecoins, post-quantum cryptography, blockchain, migration, quantum computing

1 Introduction

Stablecoins have become a critical settlement layer for the digital-asset economy. They are used for exchange liquidity, DeFi collateral, cross-border transfers, payment settlement, and increasingly as programmable cash-like instruments in tokenized finance. Recent SoK-style work emphasizes that their risk profile is not reducible to price stability: stablecoins combine payment-system design, legal obligations, governance, reserve management, smart-contract control, and cross-chain deployment choices [70, 72, 120]. This paper studies a dimension that remains under-systematized in that literature: the post-quantum security of stablecoin systems.

The problem is especially acute because stablecoin value is often concentrated behind a small number of accounts. A large fiat-backed issuer may rely on a relatively small set of treasury, minting,

burning, pausing, blacklisting, upgrade, custody, oracle, and bridge keys. A crypto-collateralized stablecoin distributes some authority through governance, but still depends on oracle signatures, liquidation mechanisms, emergency controls, and the cryptography of the host chain. A bridged stablecoin adds lockboxes, relayers, committees, light clients, and cross-chain attestations. One successful key extraction can therefore affect supply, redemption, or liquidity far beyond the balance of an ordinary wallet.

Stablecoins also separate the actor able to correct a vulnerability from the parties that bear its cost. A host-chain community controls account and consensus changes; an issuer controls mint and freeze roles; a bridge operator controls a wrapped representation; holders, exchanges, lending protocols, and redeemers may absorb the resulting loss. We call this separation the *authority–liability gap*. It is central to post-quantum stablecoin migration because a technically available upgrade may still be delayed or incomplete when authority, incentives, and legal obligations are distributed across different organizations.

Quantum computing changes the threat model for the public-key primitives used by blockchains. Shor’s algorithm threatens RSA, ECDSA, Schnorr, EdDSA, BLS-style pairing-based signatures, and other constructions based on factoring or discrete logarithms, while Grover’s algorithm reduces the security margin of symmetric search and hash-based primitives. Although the timeline for a cryptographically relevant quantum computer (CRQC) remains uncertain, recent resource estimates for `secp256k1` distinguish at-rest and on-spend attacks and continue to refine the required logical-qubit and runtime estimates [11, 75]. This distinction matters for stablecoins because issuer, bridge, oracle, and custody keys are long-lived, repeatedly used, and easy to identify.

The operational urgency is not determined solely by the expected date of a CRQC. Migration is a multi-year process: standards must mature, libraries and HSMs must support new primitives, custodians and wallets must implement new formats, contracts may need precompiles or new verification paths, and governance processes must coordinate changes without disrupting redemption or settlement. General migration work therefore stresses cryptographic inventories, hybrid deployment, and crypto-agility [15, 62, 84, 88]. For a stablecoin, however, a cryptographic inventory is also a financial-control inventory: every key or primitive maps to supply control, reserve movement, bridge liquidity, redemption, privacy, or governance.

Recent protocol work makes the coordination problem concrete. Zcash has proposed recoverability hooks for Orchard notes;

Bitcoin proposals address new output types and the eventual treatment of legacy signatures; Ethereum proposals consider ML-DSA precompiles, native key delegation, and a broader execution/consensus/data-layer roadmap; issuer-controlled systems such as Circle’s CCTP and xReserve expose cross-chain attestation and deprecation surfaces; and Circle’s post-quantum roadmap sets out a phased issuer plan spanning contracts, custody, a new host chain, and account recovery [17, 18, 41, 42, 46, 50, 60, 73, 79]. These proposals solve different parts of the problem. None by itself migrates the entire stablecoin stack.

Problem statement and scope. This paper presents a Systematization of Knowledge (SoK) on *post-quantum stablecoins*. We study how stablecoin systems can preserve minting authority, reserve management, transfers, bridge-backed supply, privacy, finality, and redemption against quantum-capable adversaries. Our focus is not a new cryptographic primitive or a prediction of the CRQC date. We instead systematize which stablecoin functions depend on which assumptions, who can migrate them, which losses propagate across organizational boundaries, and which protections can be deployed before host chains complete their own upgrades.

Several mechanisms studied here, including store-now-decrypt-later exposure, HSM migration, threshold authorization, and API security, also arise in other high-value financial systems. Stablecoins are nevertheless a useful exemplar because a single monetary claim composes issuer-controlled privileges with host-chain authentication and finality, bridges and oracles, custody and exchange infrastructure, and user-held keys. The actors able to migrate these components are often different from the parties that bear losses when they fail. We therefore treat stablecoins both as the primary object of study and as a concrete instance of multi-actor cryptographic migration in networked financial systems.

Contributions. We make four contributions. First, we develop a stablecoin-centric threat model that maps quantum capabilities to issuer-key forgery, wrapped-supply inflation, oracle and governance manipulation, long-range history rewriting, proof failure, and retroactive disclosure. Second, we systematize cryptographic dependencies and control surfaces, including the authority–liability gap between migration authority and loss bearing. Third, we classify migration choices by control surface, deployment layer, and cryptographic strategy, and apply the taxonomy to current proposals and a staged migration plan. Fourth, we deepen the research agenda around missing stablecoin functionality, operation-specific security and cost, dormant and wrapped supply, private and compliance-enabled transfers, measurement, and regulatory continuity.

Method. We reviewed peer-reviewed and archival research, standards and government guidance, blockchain improvement proposals and roadmaps, and issuer or open-source documentation. We use standards and peer-reviewed results for cryptographic claims; draft EIPs, BIPs, and ZIPs as evidence of active design directions; and issuer documentation to identify deployed control structures.

To make the coverage auditable at the category level, we organize the evidence around the stablecoin functions and control surfaces used throughout the paper: account authentication; mint/burn, treasury, custody, and upgrade authority; bridges and oracles; governance and consensus/finality; rollups and privacy systems; and encrypted operational channels. For each surface, we ask four questions: (i) which classical cryptographic assumption it depends on,

(ii) which quantum capability breaks that assumption, (iii) which post-quantum replacement or migration mechanism is available, and (iv) which actor and deployment layer can actually perform the migration. Recent SoKs and surveys are used to identify adjacent categories and cross-check omissions, while primary sources are preferred for technical, standards, deployment, and regulatory claims that enter the taxonomy.

Our completeness claim is therefore category-level rather than bibliographic: we aim to cover the distinct stablecoin control surfaces, attack classes, and migration authorities, not every paper or implementation of each primitive. The paper is a systems SoK rather than a quantitative meta-analysis; newly proposed schemes can change the set of candidate mechanisms without necessarily changing the threat and migration categories.

1.1 Related Work

SoKs on blockchain systems. A large body of SoK-style blockchain work has developed taxonomies for adjacent parts of the ecosystem. Layer-two and scaling SoKs classify payment channels, sidechains, rollups, sharding, and Bitcoin L2 designs [5, 59, 102, 116]. Bridge-focused SoKs analyze cross-chain validation, lock-and-mint designs, light-client verification, bridge components, architectural flaws, and exploit classes [80, 96]. Security-focused SoKs on DeFi incidents, rug pulls, and decentralization provide incident taxonomies and measurement frameworks for smart-contract and governance risk [99, 121, 122]. These works are essential for understanding the stablecoin environment, but they generally do not ask how quantum adversaries change the cryptographic assumptions of the control surfaces they classify.

SoKs on stablecoins. Recent stablecoin SoKs study stablecoins as payment instruments, programmable settlement assets, and financial infrastructure. The retail-payments SoK compares stablecoin payment arrangements with card networks and emphasizes differences in authorization, settlement, recourse, and user risk [70]. The Stablecoin LEGO SoK develops a design-risk framework based on stablecoin incidents and composability [72]. Work on stablecoins and real-world asset tokenization develops taxonomies for design, metrics, and applications [120]. These studies provide the economic and architectural context for our work, but they do not systematize cryptographic migration, quantum attacks on issuer and bridge keys, or the post-quantum status of stablecoin-specific control paths.

Post-quantum blockchains and primitives. Surveys review quantum-vulnerable blockchain primitives, post-quantum chain designs, migration strategies, and performance effects [16, 52, 56, 78, 119]. Research on threshold and aggregate signatures, adaptor signatures, VRFs, commitments, and zero-knowledge proofs provides candidate components for custody, bridges, payment channels, consensus, and privacy [3, 34, 35, 48, 112, 117]. Implementation work such as *poqeth* shows that on-chain verifier design and opcode pricing can dominate native cryptographic performance [68]. Our unit of analysis is different: we ask how these results specialize to stablecoin control, claims, and loss propagation.

Migration proposals and chain-specific readiness. Protocol proposals cover complementary pieces of migration. ZIP-2005 adds pre-crisis recoverability for Zcash Orchard notes [60]; EdDSA-chain

work preserves deployed address formats while registering post-quantum credentials [13]; Bitcoin BIP-360 and BIP-361 address new output semantics and legacy-signature sunset policy [17, 73]; and Ethereum EIP-8051 and EIP-8164 propose specialized ML-DSA verification and native EOA key delegation [46, 79]. Other ecosystems provide useful migration case studies. Sui inventories exposure in account signatures, BLS-based randomness, TLS, bridges, and zkLogin [86]. The existing zkLogin construction uses a Groth16 proof over an OIDC credential [14], while Sui’s PQ migration analysis proposes replacing both the credential signature and proof system while retaining the account address [86]. Solana reports initial Falcon implementations by Anza and Firedancer and a staged path from new PQ wallets to legacy-wallet migration, while an application-level Winternitz vault demonstrates an overlay approach [108]. Coinbase’s 2026 Quantum Advisory Council reports separately emphasize cross-chain migration and the unresolved governance of assets that never migrate [44, 71]. Circle’s post-quantum roadmap phases readiness, transition, and switch, and states which components the issuer controls and which it must leave to host chains, vendors, and contract owners [18]. We compare the principal protocol and chain proposals in Section 4.1, emphasizing which stablecoin components remain outside each proposal’s scope.

2 Background

This section introduces the stablecoin designs, control relationships, regulatory constraints, and cryptographic building blocks used throughout the paper. We provide generic formal definitions in Appendix A.

2.1 Stablecoin Designs and Control Surfaces

Stablecoins are crypto-assets designed to maintain a relatively stable value, typically by referencing an external asset, a basket of assets, or an endogenous stabilization mechanism. For post-quantum analysis, the important distinction is not only how the peg is maintained, but which entities control issuance, redemption, collateral, and administrative functions, and which cryptographic keys authorize those actions.

Fiat-backed stablecoins. Fiat-backed stablecoins, such as USDT, USDC, PYUSD, and EURC, are issued by centralized entities that hold off-chain reserves and promise redemption at a fixed reference value. On-chain, they are commonly implemented as upgradeable contracts with privileged roles for minting, burning, pausing, blacklisting, contract upgrades, or treasury movements. Circle’s public EVM implementation, for example, separates owner, proxy-owner, master-minter, pauser, and blacklister roles [40]. These roles are controlled by issuer keys, multisignature wallets, custody providers, MPC policies, or HSMs. Quantum risk is therefore concentrated in a small number of high-value control accounts.

Crypto-collateralized stablecoins. Crypto-collateralized stablecoins, such as DAI and LUSD, are backed by over-collateralized positions in volatile crypto-assets locked in smart contracts. Their security depends on contract correctness, liquidation mechanisms, oracle integrity, governance, keeper infrastructure, and the cryptography of the host chain. They inherit user- and validator-key risk from the underlying chain while adding protocol-specific exposure

through oracle signers, governance keys, emergency shutdown mechanisms, and collateral contracts.

Algorithmic and hybrid designs. Algorithmic stablecoins attempt to maintain a peg through supply expansion and contraction, arbitrage incentives, seigniorage-style mechanisms, or multi-token structures. Historical examples include Basis Cash and TerraUSD (UST), while hybrid systems such as FRAX combined collateral with algorithmic mechanisms. These systems often rely heavily on governance keys, oracle inputs, liquidity-management contracts, and upgrade paths. Quantum compromise of those controls can destabilize the peg without directly stealing reserve assets.

Bridged and wrapped stablecoins. Stablecoins are deployed across chains through native issuance, canonical bridges, third-party bridges, and wrapped representations. In a lock-and-mint design, tokens are escrowed on a source chain and a corresponding representation is minted on a destination chain after a committee, validator set, oracle, or light client authenticates the source event. Burn-and-mint systems authorize issuance or release after a source-chain burn. The stablecoin therefore depends on bridge signers, message formats, source-chain finality, relayers, lockboxes, and destination contracts. A forged attestation can create unbacked wrapped supply or release locked value.

2.2 Control, Settlement, and Claims

A stablecoin is not a single contract. We model it as three coupled layers. The *control plane* changes supply or the rules governing it: mint and burn keys, treasury operations, pause and blacklist roles, proxy upgrades, governance, oracle administration, and bridge attestation. The *settlement substrate* authenticates users and orders transactions: host-chain accounts, validator or finality signatures, data-availability commitments, rollup proof systems, sequencers, light clients, and cross-chain verification. The *claim and distribution layer* contains holders, custodians, exchanges, DeFi protocols, payment applications, redemption channels, and wrapped representations. Parties in the last layer often absorb losses even when they do not control the failed component.

Table 1 makes the resulting authority–liability gap explicit. A technically available migration may still fail because the actor able to deploy it lacks the incentive, legal authority, or coordination channel to protect the principal loss bearer.

2.3 Regulatory Constraints on Migration

Regulation does not select a post-quantum algorithm, but it constrains acceptable migration behavior. MiCA requires governance and ICT controls, business continuity, recovery and orderly-redemption plans, and par redemption for e-money tokens; relevant obligations also apply to significant e-money tokens through Article 55 [51]. In the United States, the GENIUS Act requires one-to-one reserves and disclosed redemption procedures, directs regulators to establish operational and information-technology risk standards, and requires issuers to retain the technical capability to comply with lawful orders that may seize, freeze, burn, or prevent transfers [115]. The OCC’s February 2026 proposal addresses redemption, risk management, custody, audits, and operational

Control surface	Stablecoin consequence	Actor able to migrate	Principal loss bearer	Dependency that may block migration
Mint, burn, treasury, upgrade	Unauthorized supply, reserve movement, freeze, or contract replacement	Issuer, DAO, custodian	Holders, redeemers, issuer	Host-chain verifier, HSM/MPC support, governance delay
Immutable contracts verifying ecrecover signatures	Forged permits and gasless transfers into unupgradeable DeFi, custody, and payment contracts	Host chain (hard fork replacing ecrecover)	Contract owners and their users	No upgrade path; 65-byte signature ABI; PQ keys require a registry [18]
Oracle and liquidation	False collateral state, liquidations, or peg failure	Oracle network, protocol governance	Vault users, liquidity providers, holders	Aggregation, update frequency, contract gas
Bridge lockbox and attestation	Unbacked wrapped supply or release of locked assets	Bridge operator, issuer, source/destination chains	Wrapped-token holders, exchanges, DeFi protocols	Source finality, committee signatures, redemption coordination
Host-chain accounts and consensus	User theft, validator forgery, history rewriting	Chain governance and client implementers	Users and all applications on the chain	Hard fork, wallet support, light clients, dormant accounts
Rollup and privacy systems	Invalid state transitions, false compliance proofs, retroactive disclosure	Rollup or privacy-system operator	Users, issuers, regulated intermediaries	Proof replacement, recursion, wallet proving cost
Dormant and inaccessible balances	Persistent exposed supply or coercive freeze/recovery	User, issuer, or chain depending on design	Dormant holder; active holders through confidence loss	Lost keys, legal ownership, recovery proof, deadline policy

Table 1: Stablecoin control surfaces separate migration authority from financial liability.

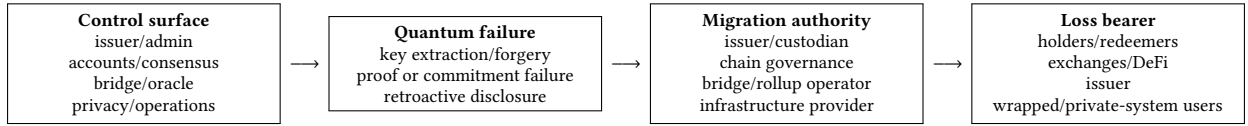


Figure 1: Stablecoin quantum risk is compositional: a cryptographic failure propagates through a control surface, but the actor able to migrate that surface and the party bearing the resulting loss may differ.

Source	Requirement	Migration consequence
MiCA Art. 34	Governance, ICT controls, continuity	Key and contract migration must be inventoried, tested, and auditable.
MiCA Arts. 46–47, 49, 55	Recovery, orderly redemption, par deemability	Freezes, reissuance, and claim contracts must preserve timely and equitable redemption.
GENIUS Act §4	Reserves, disclosed redemption, operational/IT risk	A PQ incident is an operational-risk and disclosure event, not only a protocol bug.
GENIUS Act §4(a)(6) and OCC proposals	Lawful orders, custody, audit, AML/sanctions	Migration must preserve required freeze, burn, screening, blocking, and reporting controls.

Table 2: Examples of regulatory duties that constrain stablecoin migration.

backstops [98]; a June 2026 proposal separately addresses BSA/AML and sanctions programs [97].

These provisions sharpen the stablecoin-specific problem. A chain-level proposal that abandons old accounts may conflict with an issuer’s redemption duties. Conversely, a migration that preserves user signatures but removes pause, blacklist, recovery, or lawful-order capability may be unacceptable for a regulated issuer. Regulation therefore constrains recovery semantics, authority, audit evidence, and continuity rather than merely providing external motivation.

2.4 Cryptographic Primitives, Quantum Vulnerabilities, and Post-Quantum Candidates

Hash functions. Hash functions support transaction identifiers, Merkle trees, state commitments, nullifiers, proof systems, and address derivation. Grover’s algorithm gives a quadratic preimage speedup, while BHT gives a stronger asymptotic collision attack under quantum-memory assumptions [30, 58]. Grover parallelizes

poorly, so 256-bit hashes retain roughly a 128-bit generic post-quantum margin. Hash-based signatures such as SLH-DSA, XMSS, and LMS, and transparent STARK systems, inherit security primarily from these properties [20, 31, 61, 63]. Stablecoin systems should therefore prioritize public-key migration rather than replace well-sized hash functions indiscriminately.

Digital signatures. ECDSA, Schnorr, EdDSA, RSA-PSS, and BLS signatures rely on factoring, discrete-logarithm, or pairing assumptions and fall to Shor’s algorithm [22, 28, 104, 105]. Once a public key is exposed, a CRQC can recover the secret and create signatures indistinguishable from honest ones. This threatens not only future transactions but also the evidentiary value of historical signatures, reserve attestations, and audit logs. Stablecoin mint, treasury, bridge, oracle, and upgrade keys are typically in the at-rest regime because their public keys are long-lived and visible [11].

NIST has finalized ML-DSA and SLH-DSA and is continuing standardization of FN-DSA, based on Falcon [90, 91, 94]. ML-DSA has kilobyte-scale public keys and signatures and is a plausible default for low-frequency issuer administration. SLH-DSA offers conservative hash-based security at much larger signature sizes. Falcon/FN-DSA is more compact but has demanding implementation and side-channel requirements. For tightly controlled low-frequency keys, NIST SP 800-208 also approves the stateful hash-based LMS and XMSS families and stresses careful state management and hardware-backed key handling; this profile is better matched to treasury or recovery controls than to retail transfers [45]. In May 2026, NIST advanced nine additional signature candidates, FAEST, HAWK, MAYO, MQOM, QR-UOV, SDitH, SNOVA, SQIsign, and UOV, to a third evaluation round [93]. None of these developments provides a drop-in replacement for BLS-style non-interactive aggregation.

Multisignatures and threshold signatures. Stablecoin custody, issuer administration, exchange wallets, bridge committees, and validator sets rely on distributed authorization. Threshold ECDSA, FROST-style Schnorr, and threshold BLS remain vulnerable because Shor recovers the aggregate secret from the aggregate public key; the attacker need not compromise each share [12, 55, 66]. Lattice multisignatures and threshold signatures exist [3, 37, 47], and recent work specifically targets threshold ML-DSA through MPC and identifiable-abort constructions [24, 29]. These results narrow the primitive gap, but stablecoin deployment still requires dynamic committees, signer accountability, HSM/MPC support, key rotation and recovery, compact verification, and audit evidence.

Key exchange and authenticated channels. Issuer-custodian APIs, reserve operations, bank and exchange connections, oracle feeds, node links, and incident-response channels depend on encrypted communication. DH/ECDH, ECIES, and RSA-OAEP lose their security under Shor [107]. This creates store-now-decrypt-later exposure for archived operational and customer data. ML-KEM is standardized, and HQC has been selected for ongoing standardization as a backup KEM [89, 92]. Hybrid KEMs can therefore be deployed in issuer infrastructure before host-chain account formats change. An active IETF standards-track Internet-Draft defines X25519MLKEM768, SecP256r1MLKEM768, and SecP384r1MLKEM1024 for TLS 1.3, providing a concrete hybrid migration path for issuer-custodian and issuer-bank channels while the document remains work in progress [67].

Randomness, VRFs, and leader election. VRFs and randomness beacons support validator or committee selection, auctions, and some governance and liquidation mechanisms. EC-VRFs and threshold-BLS beacons inherit discrete-log or pairing risk; a recovered key makes future outputs predictable and can permit bias or control [82, 87]. Symmetric-primitive and lattice-based post-quantum VRFs have been proposed [1, 35], but proofs are larger and integration with high-throughput consensus and light-client sampling remains immature.

2.4.1 Privacy and Advanced Functionality.

Zero-knowledge proofs. Groth16, PLONK with KZG, Bulletproofs, and Halo-style systems derive soundness from pairing or discrete-log assumptions; Shor can therefore enable accepting proofs for false statements, including invalid rollup transitions or creation of unbacked shielded balances [26, 33, 53, 57, 109]. STARKs rely primarily on hash commitments and FRI-style testing and are treated as post-quantum under appropriate hash parameters [20]. Lattice-based SNARKs and zero-knowledge arguments, and MPC-in-the-head systems such as Ligerio, Aurora, and Picnic, provide alternatives with different proof-size, recursion, and verifier-cost trade-offs [6, 8, 21, 38, 49, 54, 77, 95]. These costs matter directly for private stablecoin transfers, reserve proofs, compliance proofs, and rollup settlement.

Commitments. Pedersen commitments are statistically hiding but computationally binding under the discrete-log assumption; Shor breaks binding and permits inconsistent openings [100]. This

can invalidate confidential balances or reserve proofs without compromising an issuer signing key. KZG commitments similarly inherit pairing risk, while hash-based commitments retain a post-quantum margin at 256-bit parameters. Lattice commitments integrate with lattice proof systems but have different proof and verifier costs [9]. The relevant migration question is therefore the entire proof-and-commitment stack, not the commitment in isolation.

Encryption and AEAD. Symmetric encryption and AEAD face generic Grover-style key search; 256-bit keys provide a practical post-quantum baseline. Under superposition access to a keyed primitive, Simon-style attacks can break some MAC and mode constructions, although such access is unrealistic for ordinary stablecoin attackers [64]. Public-key encryption based on ECIES or RSA falls under Shor. A post-quantum design should therefore use ML-KEM or a hybrid KEM with 256-bit AEAD and should consider forward secrecy to reduce the value of archived traffic [19].

Exotic signatures (ring, blind, adaptor, and aggregate). These appear in stablecoin privacy layers, bridge attestations, payment channels, and atomic swaps.

Ring signatures [103] let a signer sign on behalf of a ring $R = \{pk_1, \dots, pk_n\}$ with **unforgeability** and **anonymity** (the signer's identity is hidden within R). DL-based constructions (LSAG, ML-SAG in Monero) lose both under Shor: once any ring member's sk is recoverable, the adversary can both forge and deanonymize, implying *retroactive deanonymization* of historical transactions and any ring-based stablecoin pool. PQ candidates: lattice ring signatures (Raptor [74], lattice RingCT [113, 114]) and code-based variants.

Blind signatures (e-cash, confidential withdrawals) require **blindness** and **one-more unforgeability**. For DL-based schemes, Shor enables recovery of the signing key and therefore destroys unforgeability. The effect on blindness is construction-dependent: schemes with statistical blindness can retain that property even after the signing key becomes recoverable. Lattice blind signatures [2, 23] are available but with sizes far above ECDSA-based variants.

Adaptor signatures [10] tie signature publication to revealing a witness w for $Y = f(w)$, requiring **pre-signature adaptability**, **witness extractability**, and **aEUF-CMA**. In EC-based constructions w is a discrete log, so Shor extracts w directly from $Y = g^w$ without ever observing a signature; breaking the entire construction. PQ candidates target payment-channel networks [48, 112].

Aggregate signatures. BLS [27, 28] compresses n signatures over distinct messages and keys into a single 48-byte element; all variants are broken by Shor. Lattice sequential aggregate signatures [117] exist but are limited in non-interactive aggregation and rogue-key resistance. This is among the most pressing open problems for post-quantum bridge attestations.

3 Threat Model and Quantum Attack Surface

This section identifies quantum-relevant threats to stablecoin systems. We distinguish *capabilities* (what the adversary can compute), *attack patterns* (how those capabilities are used), and *stablecoin control surfaces* (which assets or operations are affected).

3.1 Adversary Model and Capabilities

We formalize the adversary in three layers: classical capabilities, quantum capabilities, and the time horizon over which capabilities accumulate.

Classical adversary. Let $\mathcal{A}_c$ denote a PPT adversary. We assume $\mathcal{A}_c$ has the following abilities, all of which are realistic for present-day attackers on public blockchains:

- **Public-ledger observation:** read all on-chain state, including transactions, contract code, public keys, signatures, Merkle proofs, rollup state commitments, bridge attestations, and oracle messages.
- **Transaction submission:** post arbitrary transactions; perform front-running, sandwiching, and MEV; deploy contracts.
- **Node and P2P operations:** run validators, RPC providers, relayers; observe and archive mempool traffic and gossip meta-data.
- **Network archival:** passively record encrypted off-chain traffic (TLS sessions, custodian APIs, oracle feeds, bridge relayer traffic). This is the substrate for store-now-decrypt-later attacks. For off-chain SNDL, the adversary needs a ciphertext-recording vantage point, such as an ISP or transit path, enterprise or cloud-network infrastructure, a compromised network appliance, or service-side packet logging; endpoint compromise is a stronger capability and is not assumed. Public on-chain ciphertexts require no privileged vantage point because any observer can archive them.
- **Selective corruption:** compromise or bribe a bounded subset of off-chain participants (bridge committee members, oracle signers, custodians, validator operators). We do not assume any single party is fully corrupted.

Quantum adversary. The quantum adversary $\mathcal{A}_q$ is a QPT machine that additionally holds (or has time-shared access to) a CRQC sufficient for the workloads below.

- **Shor’s algorithm** [105]: given a target public key $pk \in \mathbb{G}$ for any blockchain-relevant group $\mathbb{G}$ (secp256k1, secp256r1, Curve25519, BLS12-381), recover the corresponding secret key sk in time $\text{poly}(\log |\mathbb{G}|)$. Recent circuit estimates put the logical-qubit requirement for 256-bit prime-field ECDLP at roughly 10^3 . For secp256k1, Babbush et al. [11] report time-space trade-offs using at most about 1,200 logical qubits and 90 million Toffoli gates, or about 1,450 logical qubits and 70 million Toffoli gates. More recent work by Luo et al. [75] gives an 835-logical-qubit construction for a 256-bit prime-field curve. These are *logical* resource counts; the number of physical qubits required for a fault-tolerant implementation is substantially larger and depends on the error-correction architecture, physical error rate, and target runtime.
- **Grover’s algorithm** [58]: $\Theta(2^{n/2})$ queries to invert an arbitrary n -bit function. Parallel speedup is only $\sqrt{k}$ in the number of parallel oracles, which substantially limits Grover’s threat at 256-bit hash output sizes.
- **Simon’s algorithm / quantum chosen-input attacks** [106]: relevant against some MACs and stream ciphers under *superposition* queries to the keyed primitive. In practice, blockchain

attackers cannot obtain such queries against issuer infrastructure, so the threat is mostly theoretical for stablecoins.

Remark 1 (Granularity of quantum compromise). Quantum capability is not all-or-nothing. We distinguish three regimes:

- (1) **Targeted offline key extraction:** the adversary can afford one Shor run per high-value target. This already destroys treasury and bridge keys whose public keys are static and known.
- (2) **Batched extraction:** the adversary can run Shor against many keys per day. All exposed EOAs become extractable; the bottleneck shifts to ranking targets by value.
- (3) **Online race-the-mempool:** the adversary intercepts a transaction at broadcast time, extracts sk from the revealed pk , and submits a competing transaction before the original confirms. Even short windows (12–15s on Ethereum) become feasible once Shor runtimes drop into the seconds range.

For stablecoins, the at-rest regime is already devastating because issuer, bridge, and oracle keys live in static, on-chain addresses; the on-spend regime is the regime ordinary user wallets need to worry about.

Time horizon. A useful planning model is *Mosca’s inequality* [85]: a cryptosystem must be considered insecure if $X + Y > Z$, where X is the shelf-life of the protected data, Y is the migration time, and Z is the time until a CRQC is operational. For stablecoins:

- X is years to decades: reserve attestations, compliance records, and shielded transaction histories may need to remain unforgeable or private for very long horizons.
- Y is large because stablecoins span issuer infrastructure, smart contracts, bridges, rollups, custodians, exchanges, wallets, and host-chain consensus, and migration of each layer requires its own governance process.
- Z is uncertain but trending downward: recent resource estimates [11, 75] continue to lower the qubit and time cost of such attacks.

3.2 Stablecoin Attack Patterns

We now systematize the attack patterns that follow from the capabilities of Section 3.1. Each pattern is stated in terms of the target property, attacker capability, goal, and impact.

ATTACK 3.1 (AT-REST KEY EXTRACTION AND FORGERY). *Target property:* EUF-CMA security of the deployed signature scheme. *Capability:* Shor on already-revealed pk . *Goal:* produce signatures σ on attacker-chosen messages m authenticated by sk , without ever observing legitimate signatures.

The set of *at-rest exposed* stablecoin keys typically includes treasury and mint multi-sig signer keys; proxy-admin / upgrade keys; pause and blacklist authorities; bridge committee keys; oracle signer keys; custodian co-signing keys; and host-chain validator keys. Each is a *concentrated control surface*: one forged signature may mint supply, freeze balances, replace implementation logic, push a malicious oracle update, or finalize a malicious checkpoint.

ATTACK 3.2 (KEY EXTRACTION RACE (ON-SPEND)). *Target:* account-level signatures whose pk is revealed at spending time. *Capability:* fast Shor extraction and mempool monitoring. *Goal:*

extract sk from the broadcast pk and submit a higher-fee replacement transaction before the original confirms.

For stablecoins, this primarily threatens user holdings. The system-level impact is bounded by chain throughput, but the individual-user impact is total loss.

ATTACK 3.3 (RETROACTIVE DISCLOSURE - STORE-NOW DECRYPT-LATER (SNDL) AND PRIVACY LOSS). **Target property:** confidentiality of archived ciphertexts (IND-CCA / IND-CPA of past KEM/PKE traffic) and anonymity / hiding of on-chain privacy mechanisms (ring signatures, shielded notes, viewing keys, ZK witness-hiding). **Capability:** archive ciphertexts and on-chain artifacts now; later apply Shor to the underlying DLP / pairing / factoring assumption. **Goal:** recover plaintexts of past communications and reconstruct the historical transaction graph of past private transfers.

For the off-chain branch, passive recording therefore requires network visibility but not plaintext or endpoint access; for the on-chain branch, ordinary public-ledger access is sufficient to archive the relevant artifacts.

This pattern unifies two related threats that share an “archive now, break later” structure but affect different surfaces. *Off-chain SNDL* on encrypted issuer–custodian APIs, redemption queues, and compliance traffic exposes signing-ceremony schedules, reserve-rebalancing instructions and bank references, KYC envelopes, and bridge relay topology, enabling timed treasury attacks, phishing of banking partners, regulatory harm, and targeted compromise of bridge committees, all without any on-chain action. *On-chain retroactive privacy loss* affects stablecoins routed through ring-based pools (Monero-style), shielded protocols (Zcash, Aztec, Railgun), or privacy-preserving rollups: once the underlying assumption falls, payer–payee links, amounts, timing, and DeFi positions become reconstructible years after the transactions appeared private. The harm in both sub-cases is informational and *cannot be repaired by re-issuance or freezing*: the data is already out, and the cryptographic break is permanent. Privacy mechanisms also differ in their assumptions: the Circle Research–Inco confidential-token design uses fully homomorphic encryption over balances and amounts, whereas note-based systems combine commitments, zero-knowledge proofs, and encrypted note data [43]. The assessment must therefore inventory the actual privacy construction rather than infer security from the token interface.

ATTACK 3.4 (BRIDGE AND WRAPPED-ASSET FORGERY). **Target property:** EUF-CMA or threshold-unforgeability of the bridge attestation scheme. **Capability:** Shor against committee public keys or aggregate BLS keys. **Goal:** produce attestations for lock/burn events never occurred.

A successful forgery on a lock-and-mint bridge mints unbacked wrapped stablecoin on the destination chain; on a burn-and-mint bridge it releases native value without a corresponding burn. Because wrapped assets are often traded as fungible claims, the attack can propagate through exchanges, AMMs and lending platforms before reconciliation detects the mismatch. Circle xReserve illustrates the dependency structure of a modern issuer-backed interoperability system: a Circle-deployed reserve contract, an API-issued attestation, and partner-chain mint/burn logic jointly determine

issuance and redemption [42]. A post-quantum migration must cover all three rather than only the destination token.

ATTACK 3.5 (ORACLE AND GOVERNANCE MANIPULATION). **Target property:** signature unforgeability of oracle reports or governance votes; ZK soundness for off-chain attested data; VRF uniqueness/pseudorandomness for auctions or committee sampling. **Capability:** Shor on signer/voter keys or on pairing assumptions. **Goal:** induce false price updates, unjustified liquidations, or replacement of oracle/governance sets.

For crypto-collateralized and hybrid stablecoins, oracle and governance forgery can trigger mass liquidations, conceal undercollateralization, or replace peg-maintenance modules.

ATTACK 3.6 (COMMITMENT EQUIVOCATION IN CONFIDENTIAL BALANCES). **Target property:** computational binding of a Pedersen, KZG, or related commitment used for confidential balances or proofs of solvency. **Capability:** Shor on the underlying DLP or pairing assumption. **Goal:** open the same commitment to inconsistent values.

This pattern does not require a signing key. A DLOG break can let proofs of solvency overstate assets, or let confidential-balance systems equivocate about balances, whenever binding relies on discrete-log assumptions.

ATTACK 3.7 (SOUNDNESS BREAK IN VALIDITY PROOFS). **Target property:** computational soundness of pairing-based or DLP-based SNARKs. **Capability:** Shor against the soundness assumption. **Goal:** produce accepting proofs π for false statements $x \notin \mathcal{L}$.

Direct impacts include invalid rollup state transitions, invalid shielded-pool balance updates, and forgeable compliance or proof-of-reserves proofs.

Summary of attack patterns. Table 3 summarizes the patterns, the security property they target, and the dominant stablecoin control surface they affect.

3.3 Layered Composition of Threats

The attacks above do not occur in isolation: the same cryptographic break can appear at different layers of the stablecoin stack. We therefore summarize how the labeled attacks compose across the stablecoin layer stack.

Application layer. At the stablecoin-application layer, the dominant risks are concentrated control surfaces: mint, burn, pause, blacklist, treasury, upgrade, oracle, governance, custody, and bridge keys. The primary attack is key extraction and signature forgery against already exposed high-value public keys (Attack 3.1). Bridge-controlled stablecoin supply is exposed through forged bridge attestations and wrapped-asset inflation (Attack 3.4), while oracle and governance manipulation affects collateral ratios, liquidations, peg modules, and parameter updates (Attack 3.5). If the stablecoin or its surrounding infrastructure uses confidential balances, proof-of-reserves commitments, shielded transfers, or compliance proofs, then commitment equivocation and proof-system soundness attacks also become application-layer concerns (Attacks 3.6 and 3.7). A further application-layer surface is the ecrecover-based verification of off-chain authorizations such as EIP-2612 permits and

Pattern	Property broken	Stablecoin surface
A. At-rest extraction	EUF-CMA of signature	Mint / treasury / admin / oracle / bridge keys
B. On-spend race	EUF-CMA at key disclosure	User wallets and dormant balances
C. Retroactive disclosure	IND-CCA of past KEM/PKE; anonymity / hiding of privacy schemes (offline)	Custody / compliance / API traffic; shielded stablecoin history
D. Bridge forgery	Threshold / aggregate unforgeability	Wrapped supply and lockboxes
E. Oracle / governance	Report/vote unforgeability	Peg logic, liquidation, parameter updates
F. Commitment equivocation	Commitment binding	Confidential balances, proof-of-reserves
G. ZK soundness	Proof-system soundness	Rollups, shielded pools, compliance proofs

Table 3: Quantum-enabled attack patterns for stablecoin systems.

EIP-3009 transfers. The stablecoin contract itself may be upgradeable, but most contracts that consume these signatures are not, so Circle’s post-quantum roadmap identifies a host-chain replacement of ecrecover as the only remedy and places remediation responsibility on contract owners [18].

Blockchain stack. At the blockchain stack layer, stablecoins inherit account authentication, validator signatures, finality, light-client verification, bridge verification, and rollup settlement from their host chains. User balances are exposed through on-spend key extraction when a public key is revealed only at transaction time (Attack 3.2), while validators, sequencers, light-client committees, and exposed account or contract-admin keys fall under at-rest key extraction (Attack 3.1). Long-range proof-of-stake rewriting is not a separate primitive attack; it is a composition of at-rest key extraction against historical validator keys with the chain’s finality and weak-subjectivity assumptions. Similarly, rollup or bridge failure may arise from forged attestations (Attack 3.4) or from a soundness break in pairing- or DLP-based validity proofs (Attack 3.7). Thus, a stablecoin contract can use PQ-safe issuer controls while still depending on quantum-vulnerable host-chain accounts, validator signatures, light-client proofs, or rollup verifiers.

Network, metadata, and privacy layer. Stablecoin operators also depend on off-chain encrypted channels, APIs, custody procedures, banking partners, customer-support systems, compliance databases, and private-payment layers. Retroactive disclosure through store-now-decrypt-later and privacy loss (Attack 3.3) dominates this layer. It can reveal issuer–custodian communications, redemption queues, reserve movements, KYC envelopes, bridge-relayer topology, or shielded stablecoin flows. These failures may not directly mint or steal tokens, but they can expose users, enable targeted compromise, undermine compliance guarantees, and permanently reveal historical payment information.

Cross-layer implication. Lower-layer quantum risk propagates upward. A PQ-secure issuer key does not protect users if the host chain’s account signatures can be forged via Attack 3.2; a PQ-secure bridge committee does not protect wrapped supply if the source-chain finality evidence can be rewritten via Attack 3.1; and a PQ-secure token contract does not preserve privacy if the surrounding privacy layer is vulnerable to Attack 3.3, Attack 3.6, or Attack 3.7. Conversely, issuers can still reduce risk before full base-layer migration by hardening custody, admin, bridge, oracle, and

off-chain communication paths. The remaining exposure follows the authority–liability gap in Table 1: the actor able to migrate one layer may not control the layer that fails or bear the resulting loss. This layered view motivates the migration strategies in Section 4.

4 Taxonomy and Migration Strategies

This section provides the main systematization framework of the paper. The *control-surface* dimension identifies who has authority to migrate a component, the *migration-layer* dimension identifies where the change must occur, and the *cryptographic-strategy* dimension identifies how quantum resistance is introduced. Used together, the dimensions expose incomplete migrations: a proposal may introduce a post-quantum primitive while leaving the responsible actor, lower-layer dependency, or legacy state unspecified.

We first summarize the cryptographic dependencies of stablecoins. Table 4 records each primitive’s role, representative uses, and current post-quantum direction. Section 3 gives the stablecoin consequences of failure.

Dimension 1: Control surface. The control-surface dimension asks who has practical authority to change a component. **Issuer-controlled** components include HSM and MPC policies, smart-contract admin keys, treasury wallets, mint and burn roles, pause and blacklist roles, and emergency multisigs. **Host-chain-controlled** components include account formats, consensus signatures, base-layer randomness, precompiles, transaction validity, and protocol-level proof systems. **Ecosystem-controlled** components include custodians, exchanges, oracle providers, bridge operators, relayers, wallet vendors, auditors, and rollup sequencers. A migration plan that names an algorithm but not the actor responsible for deployment is incomplete.

Dimension 2: Migration layer. The migration-layer dimension asks where quantum resistance is introduced. **Infrastructure** changes cover HSMs, MPC platforms, signing ceremonies, encrypted APIs, redemption procedures, and compliance systems. **Application overlays** include smart-contract wallets, PQ-controlled vaults, hybrid admin gates, claim contracts, and bridge-attestation contracts. **Bridge/rollup-layer** changes cover lockboxes, cross-chain messages, sequencer authentication, proof systems, withdrawal bridges, and data availability. **Base-layer** changes cover native account and validator signatures, finality, randomness, light-client verification, gas accounting, and precompiles. Lower-layer

Primitive	Functionality	Blockchain examples	Post-quantum candidates / status
Hash functions	Identities, Merkle trees, PoW, commitments, transaction identifiers	SHA-256, RIPEMD-160, Keccak-256, BLAKE2, Merkle trees [81]	Retain modern hashes with sufficient output length; use 256-bit outputs for long-lived commitments and nullifiers
Digital signatures	Account authentication, admin actions, validator messages, contract calls	ECDSA, Schnorr [104], EdDSA [22], BLS [28]	ML-DSA and SLH-DSA are standardized [90, 91]; FN-DSA/Falcon standardization and nine additional signature candidates remain in progress [93, 94]
Multisignatures	Custody, governance, bridge committees, issuer administration	Schnorr multisig, BLS aggregation, ECDSA multisigs; lattice proposals [47]	Lattice multisignatures exist; compact aggregation, accountability, key rotation, and wallet integration remain open
Threshold signatures	Distributed custody, consensus, bridge attestation, treasury approval	Threshold ECDSA, FROST, threshold BLS	Lattice threshold signatures [3, 37]; production performance, identifiable abort, dynamic committees, and custody integration remain open
Randomness / VRFs	Leader election, committee sampling, lotteries, validator selection	Ethereum RANDAO [87]; Algorand-style VRFs [82]	Symmetric-key and lattice-based PQ VRFs [1, 35]; proof size and consensus integration remain limiting
Key exchange	Private channels, off-chain coordination, API confidentiality	ECDH, ECIES [107]	ML-KEM is standardized; HQC is under standardization as a backup KEM [89, 92]; hybrid KEMs support staged infrastructure migration
Zero-knowledge proofs	Privacy, rollout validity, compliance proofs, reserve proofs	Groth16 [57], PLONK [53], Halo/Halo2 [26, 109], Bulletproofs [33]	STARKs [20]; lattice SNARKs and ZK [6, 54, 77, 95]; verifier cost and wallet proving remain open
Commitments	Data binding, privacy, confidential balances, reserve proofs	Pedersen [100], EC and KZG polynomial commitments	Hash commitments; lattice commitments [9]; migration must be coordinated with the proof system
Encryption / AEAD	Note encryption, private memos, off-chain communications	ECIES [107], KEM+DEM, symmetric AEAD [19]	ML-KEM or hybrid KEM plus 256-bit AEAD; archived traffic remains subject to SNDL
Exotic signatures	Privacy, payment channels, swaps, anonymous authorization	Ring [103], blind [39], adaptor [10], aggregate signatures [27]	Lattice ring/blind/adaptor schemes [2, 23, 48, 74, 112]; production readiness and aggregation remain open

Table 4: Blockchain cryptographic primitives and post-quantum migration status.

risk propagates upward, but issuers can still reduce exposure in higher layers while awaiting consensus changes.

Dimension 3: Cryptographic strategy. A **hybrid** strategy requires both classical and PQ authorization or binds a classical key to a PQ key during transition. A **PQ-native** strategy removes the classical key from the relevant authorization path. **Encapsulation** places an existing asset, key, or contract behind a PQ-aware vault or wrapper. Encapsulation is deployable without changing the original token, but remains dependent on the original admin key, host chain, bridge lockbox, or finality assumptions. It is therefore a partial migration rather than an end state. A related class of measures reduces the exposure window of a classical key without introducing post-quantum cryptography: hash-and-rotate accounts that commit only to a key hash and reveal each key once, and encrypted mempools that hide a transaction until ordering [18]. These shorten the on-spend race (Attack 3.2) but do not protect at-rest keys, so we treat them as complements to a hybrid strategy rather than as a fourth strategy.

Applying the taxonomy. Issuer-controlled migration can begin with mint, burn, treasury, reserve, oracle, redemption, and emergency-administration procedures. HSM/MPC approvals, signing ceremonies, APIs, and node links can use PQ or hybrid authentication before base-layer account formats change. This does not make the final classical on-chain signature PQ-secure, but it reduces infrastructure exposure and tests key lifecycle, audit, and recovery. Where verification is available, issuers can place privileged controls in hybrid or PQ-aware contract wallets and vaults. Crypto-collateralized systems should prioritize oracle, governance, liquidation, and emergency-shutdown paths; bridged systems should prioritize attestation, source-finality, lockbox, and redemption controls.

Dormant, rollout, and wrapped state. A migration must state what happens to users who do nothing. Options include voluntary migration with incentives, redemption and reissuance, claim contracts, a freeze after a deadline, or a post-quantum recovery proof. An issuer has additional levers that a base-layer protocol lacks: it can pause contract functionality on, or withdraw support from, a host chain that misses a post-quantum deadline, and it can relocate a

copy of a frozen contract to a chain it controls for managed recovery [18]. Each option changes property and governance semantics. Rollups require separate treatment of sequencer keys, proof systems, data-availability committees, settlement contracts, and withdrawal bridges. Wrapped supply requires route-specific sunset dates, redemption windows, and rules for residual liquidity. A PQ-safe L1 account does not automatically protect L2 or wrapped balances.

4.1 Current Proposals and Deployment Directions

Table 5 applies the dimensions to recent proposals. These are drafts, roadmaps, or product-specific systems unless stated otherwise. They demonstrate migration mechanisms, but should not be read as deployed guarantees.

The Algorand and Starknet rows summarize their June 2026 technical roadmaps [7, 110]. The Circle row is the only issuer-authored plan in the table and is useful precisely because it separates the three control surfaces of Dimension 1 from one actor’s viewpoint. As issuer, Circle plans dual-mode contracts, multisig cold storage, and infrastructure key rotation; as operator of the Arc chain, it plans a signature precompile, an ecrecover replacement, and validator-signature upgrades; and it explicitly defers HSM post-quantum support, enclave attestation, wallet key derivation, remediation of immutable contracts, and the migration of more than thirty other host chains to third parties [18]. The deferred items are the authority–liability gap stated by a party on the authority side. The Ethereum proposals also show why gas figures require an execution model. EIP-8051 assumes a specialized precompile and expanded verification key, whereas EIP-8164 assigns an intrinsic protocol cost to native account authentication. Neither is the cost of verifying ML-DSA in ordinary Solidity. By contrast, *poqeth* measures full EVM verification and finds costs from hundreds of thousands to hundreds of millions of gas for the studied schemes and parameters [68]. Appendix B separates measured, proposed, and calculated figures.

Operational sequence. A practical stablecoin migration can be staged without treating the stages as independent. First, inventory

Proposal/system	Control/layer	Mechanism	What it addresses	Stablecoin limitation
Zcash ZIP-2005 [60]	Host chain; privacy	Pre-crisis recoverability hooks for Orchard notes	Preserves a future recovery route after discrete-log assumptions fail	Does not specify the final PQ proof system, issuer policy, or redemption treatment
Bitcoin BIP-360/361 [17, 73]	Host chain; outputs and governance	P2MR output plus phased legacy-signature sunset and possible recovery	Reduces exposure for new outputs and makes dormant-state policy explicit	Does not migrate stablecoin contracts or resolve coercive freeze/recovery semantics
Ethereum EIP-8051 [46]	Base layer; precompile	ML-DSA and EVM-optimized verification precompiles	Proposes 4,500-gas specialized verification	Draft gas model; expanded key representation; no account or contract migration policy
Ethereum EIP-8164 [79]	Base layer; account	Permanent ECDSA-to-ML-DSA-44 native key delegation	In-place account migration and PQ key rotation; proposes 50,000 intrinsic gas	Draft; does not migrate contracts, bridges, validators, or dormant users
Ethereum roadmap [50]	PQ Execution, consensus, data	PQ verification, account agility, hash-based validators, proof aggregation	Treats migration as a multi-layer program rather than one signature change	Timelines, validator aggregation, and production mechanisms remain research targets
Algorand State Proofs / PQ roadmap [7, 83]	History, accounts, institutional control, consensus	Falcon-signed State Proofs and AVN verification; planned native/hybrid PQ accounts and multisig	Combines deployed historical attestations with an explicit path for treasury and custody accounts	PQ VRF and consensus signatures remain research/deployment targets; roadmap dates are forward-looking
Starknet PQ roadmap [20, 110]	Rollup, accounts, state commitments	STARK proving, native account abstraction, Pedersen-to-BLAKE2 migration, early Falcon-512 accounts	Separates proof-layer and account-layer migration; account verifiers can change without a protocol fork	Early PQ accounts are pre-audit; bridge syscalls and EIP-4844 KZG inherit Ethereum dependencies
Eddsa-chain readiness [13]	Host chain; account	Registration and transition using existing Eddsa account structure	Preserves deployed address formats while adding PQ credentials	Chain-specific; application, issuer, and bridge controls still migrate separately
Circle xRe-serve/CCTP [41, 42]	Issuer and partner chains; bridge	Issuer attestations, reserve contract, partner-chain mint/burn logic, version deprecation	Shows an issuer-controlled cross-chain migration and legacy-version sunset surface	Attestation API, contracts, partner chains, liquidity, and legacy routes must transition coherently
Circle PQ roadmap [18]	Issuer; infrastructure, application, and (on Arc) base layer	SLH-DSA-SHA2-128s precompile, dual-mode USDC contracts with a classical-disable switch, multisig cold storage, TEE privacy layer, phased switch with recovery policy	The only issuer-authored plan; states which surfaces the issuer controls and which it defers to host chains, HSM and cloud vendors, wallets, and contract owners	Base-layer parts apply to Arc only; PQ consensus signature unselected pending aggregation; PQ threshold custody deferred; enclave attestation remains classical

Table 5: Recent proposals address different parts of the post-quantum migration problem.

assumptions by monetary function—mint, burn, treasury, upgrade, pause, blacklist, redemption, oracle, governance, bridge, rollup, privacy, and settlement—and record the controlling actor and loss bearer. Second, harden issuer-controlled infrastructure and test key rotation and recovery. Third, add application, bridge, and oracle safeguards such as hybrid gates, route limits, versioned attestations, and authenticated checkpoints. Fourth, use host-chain signature agility or precompiles to remove classical authentication. Finally, define the checkpoint, claim, redemption, deadline, and loss-allocation rules for dormant and wrapped state. Auditors should retain key provenance, signer rosters, dependency graphs, test vectors, recovery exercises, and evidence of redemption continuity.

4.2 Representative Stablecoin Designs and Deployments

Table 6 maps representative stablecoin classes to the dependencies developed above. It is not a fourth taxonomy dimension; it shows how the same dimensions specialize across stablecoin designs.

The table highlights two recurring patterns. First, stablecoins inherit lower-layer cryptography even when their own contracts are simple token contracts. Second, stablecoin-specific risk is concentrated in mint keys, treasury accounts, bridge attestations, oracles, custody procedures, and upgrade paths that can affect much more value than an ordinary user key.

Cost evidence. The evidence in Appendix B supports three conclusions. Native verification latency may be acceptable for low-frequency issuer and custody actions, but calldata, data availability, aggregation, and verifier support dominate bridge, oracle, rollup,

and user-transfer costs. Available measurements permit size and some verifier-cost estimates, but do not evaluate complete stablecoin operations such as mint authorization, threshold custody withdrawal, bridge redemption, oracle retry, dormant-balance claims, private transfers, or rollup settlement. Section 5 treats this missing evidence as a research problem rather than presenting microbenchmarks as an end-to-end evaluation.

5 Research Insights, Gaps, and Open Problems

We now organize the research agenda around four stablecoin-specific findings and develop the corresponding open problems, as the preceding sections show that post-quantum stablecoin security is not obtained by substituting one signature scheme for another.

5.1 Standardized Primitives Do Not Cover Stablecoin Functions

Finding. NIST-standardized signatures and key encapsulation provide necessary building blocks for issuer administration, wallet authentication, and encrypted issuer–custodian channels. They do not cover the full functions that stablecoin systems require. The relevant unit of migration is therefore a *stablecoin function*, not an isolated primitive.

For issuer and custody keys, a replacement must support threshold policy, recovery, audit, HSM/MPC integration, and signer rotation. For bridges and oracles, it must support compact, accountable committee authorization at high message frequency. For private or compliance-enabled transfers, it must replace vulnerable commitments, proofs, encryption, and disclosure mechanisms without making mobile proving or on-chain verification impractical. For

Stablecoins	Design	Deployment	Cryptographic dependencies
USDT, USDC, PYUSD, EURC	Fiat-backed, centralized issuer	Ethereum, Tron, Solana, Base, and other chains	Account signatures, issuer roles, custody and treasury keys, upgrade controls, native or cross-chain transfer systems
DAI	Crypto-collateralized	Ethereum and L2 deployments	Accounts, governance, oracle signatures, liquidation logic, collateral contracts, keeper infrastructure
LUSD	Crypto-collateralized, low-governance design	Ethereum	Accounts, immutable or low-governance contracts, liquidation logic, price feeds
FRAX and related hybrid designs	Hybrid collateral and algorithmic mechanisms	Ethereum and L2 deployments	Governance keys, oracle feeds, AMM/liquidity logic, collateral accounting, account signatures
UST and earlier algorithmic designs	Algorithmic/seigniorage-style	Historical deployments	Governance, oracle or market mechanisms, account signatures, liquidity and arbitrage infrastructure
USDC.e and wrapped USDC/USDT variants	Bridged or wrapped representation	Bridges, rollups, sidechains, app-chains	Attestations, lockboxes, wrapped-token contracts, light clients, relayers, committee or validator signatures
Stablecoins in Aztec- or Railgun-style private systems; Circle Research-Inco design	Private or shielded transfer layer	Shielded pools, private rollups, confidential-token systems	Commitments, encryption or FHE, nullifiers, ZK proofs, viewing/disclosure mechanisms, underlying token controls [43]

Table 6: Representative stablecoin classes and their main cryptographic dependencies.

host-chain consensus, the loss of BLS aggregation becomes a bandwidth and finality problem rather than merely a larger-signature problem. Ethereum’s public post-quantum program, for example, considers hash-based validator signatures together with proof aggregation [50].

Gap: authorization suites rather than isolated schemes. Post-quantum multisignatures, threshold signatures, VRFs, adaptor signatures, and proof systems exist, but they have not yet been combined into production authorization suites for stablecoin operations. Recent threshold ML-DSA constructions based on MPC and identifiable-abort techniques narrow one part of this gap [24, 29], but they do not by themselves provide the complete custody and governance semantics required by a stablecoin deployment. A useful design must specify committee churn, identifiable abort, key recovery, audit logs, hardware assumptions, signature or proof size, verification location, and failure handling. The requirements differ across four workloads: (i) issuer and custody control, (ii) bridge and oracle committees, (iii) private and compliance-enabled transfers, and (iv) host-chain or rollup settlement. Security proofs are necessary, but insufficient if a scheme cannot reproduce the control and audit semantics of the system it replaces. Deployment evidence confirms the gap. Circle’s roadmap judges post-quantum threshold and MPC signing prohibitive in the near term across the algorithms it must support and instead moves cold storage to on-chain multisig contracts; it also warns that exporting keys from an HSM without post-quantum support in order to sign on a general-purpose CPU creates a larger classical risk than the quantum risk it is meant to address [18].

Gap: implementation and custody security. Algorithmic post-quantum security does not imply secure deployment in custody hardware. Practical side-channel work on Dilithium/ML-DSA and Falcon shows that lattice signatures introduce implementation surfaces that require dedicated hardening [65, 111]. For stablecoin issuers and custodians, evaluation should therefore include secure-element and HSM memory limits, key-generation and signing latency, masking and fault protections, key-export requirements, and compatibility with threshold or MPC custody, rather than only signature size and verifier cost.

Gap: aggregation and economic amplification. Standardized PQ signatures do not provide BLS-like non-interactive aggregation.

Posting independent signatures increases calldata, data availability, and verifier work, and the increase is amplified by bridge messages, oracle updates, validator votes, and rollup settlement. Research should compare threshold signing, sequential or interactive aggregation, proof aggregation, committee sampling, and optimistic verification under the same accountability and failure model. The objective is not simply the smallest signature; it is the lowest end-to-end cost that preserves attribution, slashing or dispute evidence, and recovery. The same constraint appears in issuer planning: Circle leaves its post-quantum consensus signature unselected pending a practical aggregate alternative to BLS, and considers STARK batch verification and fraud proofs as throughput options [18]. The fraud-proof route rests on signatures that decompose into independently checkable components, so that a validator who attests to a batch can be refuted by exhibiting one failing component; flexible signatures, which allow verification to be truncated at a chosen cost and still yield a graded validity guarantee, provide one such structure [69].

5.2 Security Level and Cost Depend on the Stablecoin Operation

Finding. Grover’s quadratic speedup does not make every hash or symmetric component equally urgent. With well-sized 256-bit primitives and poor linear parallelization, public-key authentication and loss of compact aggregation dominate the immediate migration problem. However, the appropriate post-quantum security level is operation-specific. A treasury recovery key may be used rarely but protect enormous value for decades. An oracle message may carry less value per update but be issued continuously. A retail transfer must fit wallet and fee constraints. A bridge attestation combines high value and high frequency.

Representative cost anchors. Table 7 puts the workload differences above against representative cryptographic costs. The numbers should not be compared as if they measured the same execution model: signature sizes come from standards or scheme specifications, calldata values account only for transporting the signature, and protocol-supported verification can differ by orders of magnitude from ordinary smart-contract verification. The table is therefore useful for identifying the dominant constraint for each stablecoin operation, rather than for ranking schemes by a single cost metric.

Mechanism	Key / signature size	Native or protocol support	Data / on-chain implication	Stablecoin interpretation
ECDSA / secp256k1	65-B signature	Native EVM ecrecover	3,000 gas verification; about 1,040 calldata gas [36, 118]	Current account and administrator baseline.
ML-DSA-44	pk 1,312 B; sig 2,420 B [90]	Standardized; proposed specialized Ethereum support in EIP-8051 and EIP-8164	About 38.7k calldata gas for the signature alone; verification depends strongly on execution support [36, 46, 79]	Plausible for issuer administration, mint/burn, and low-frequency treasury authorization.
ML-DSA-65	pk 1,952 B; sig 3,309 B [90]	Standardized; no deployed EVM precompile	About 52.9k calldata gas for the signature alone [36]	Illustrates the bandwidth cost of higher-security bridge, oracle, or custody authorization.
Falcon-512	pk 897 B; sig about 666 B [101]	Compact lattice signature; FND-DSA standardization is still in progress	About 10.7k calldata gas for a typical signature; no deployed EVM precompile	Attractive when bandwidth dominates, but implementation and side-channel requirements complicate custody/HSM use.
SLH-DSA	Parameter-dependent; signatures are several to tens of KB [91]	Standardized hash-based construction	An 8-KB signature alone costs over 100k calldata gas; contract verification is substantially more expensive	Better suited to infrequent recovery or emergency paths than high-frequency bridge or oracle messages.
PQ-friendly proofs	STARK and lattice-proof sizes are workload-dependent	Hash- and lattice-based constructions avoid pairing/DLP assumptions	No meaningful single gas figure: cost depends on arithmetization, recursion, aggregation, and verifier design	Relevant to private transfers, reserve/compliance proofs, and rollout settlement.

Table 7: Representative cost anchors for stablecoin-relevant classical and post-quantum primitives. Size-derived calldata costs use 16 gas per non-zero byte and exclude verification, public-key storage, aggregation, and transaction overhead. Detailed measured and proposed EVM costs appear in Appendix B.

Operation	Frequency	Value concentration	Primary constraint
Treasury or recovery	Low	Very high	Long-term assurance, audit, recovery
Mint, burn, admin	Low-medium	Very high	Direct verification, control continuity
Bridge/oracle	High	High	Aggregation, bandwidth, latency
Retail transfer	Very high	Low per transfer	Fee, wallet size, batching
Private transfer	High	Variable	Proof size, proving time, disclosure policy

Table 8: Post-quantum requirements differ across stablecoin operations.

Gap: choosing a security level. Standards bodies classify security levels against defined cryptanalytic benchmarks, whereas blockchain deployments often make cost-driven choices based on gas, bytes, bandwidth, wallet support, and validator throughput. The lowest standardized level may still be costly on-chain, creating pressure to use weaker or ad hoc constructions. Stablecoin research should select parameters from an explicit risk budget that includes value at risk, key lifetime, public-key exposure, migration latency, update frequency, and the consequences of a failed authorization. The result may legitimately differ between a cold treasury key and a high-frequency oracle, but the difference should be justified rather than inherited from unrelated conventions. Circle’s roadmap applies this reasoning explicitly: it selects level-1 SLH-DSA-SHA2-128s for signatures, which can be upgraded later, but level-3 hybrid KEMs (X-Wing, X25519MLKEM768) for encryption, because privacy lost to store-now-decrypt-later cannot be restored [18].

Gap: complete-operation benchmarks. Table 7 provides useful primitive-level cost anchors, but these measurements are not sufficient to optimize complete stablecoin operations. *poqeth* shows that EVM opcode pricing and verifier design can dominate native cryptographic speed [68]; EIP-8051 and EIP-8164 propose very different costs because they assume different protocol support and key representations [46, 79]. Calldata makes a 2,420-byte ML-DSA-44 signature roughly 37 times larger than a 65-byte ECDSA signature,

but that comparison omits aggregation, public-key storage, contract execution, and failure recovery. A complementary deployment example comes from Liquid: Blockstream deployed a SHRINCS verifier as a Simplicity spending condition on Liquid mainnet, allowing opt-in PQ protection for issued assets including stablecoins without a consensus change; transaction size is tied to the verification budget, while the peg, Confidential Assets commitments, and block-signing consensus remain classical [25]. This illustrates why verifier placement and residual dependencies belong in an operation-level benchmark.

A stablecoin benchmark suite should therefore measure complete operations: PQ mint authorization, threshold custody withdrawal, bridge attestation and redemption, oracle update and retry, user or dormant-balance migration claims, private transfer and selective disclosure, and rollout settlement. It should report gas or native verifier cost, bytes, data-availability cost, latency, signer throughput, wallet memory, HSM/MPC support, audit evidence, recovery behavior, and financial value exposed during the operation. Appendix B summarizes the current evidence and its limitations.

5.3 The Authority–Liability Gap Creates Residual and Legacy Risk

Finding. Table 1 shows that each major stablecoin control surface crosses an organizational boundary. An issuer may rotate mint keys but cannot update user accounts; a host chain may add a new account type but cannot force a bridge or oracle to adopt it; a bridge may migrate its committee while exchanges continue to trade residual wrapped supply. The actor able to mitigate the risk is often not the party that bears the loss, which creates strategic delay and incomplete protection.

Gap: cross-layer residual risk. A stablecoin can harden issuer keys while remaining exposed through accounts, consensus, a bridge, an oracle, a rollout, a custodian, or a privacy layer. Conversely, a host chain can add PQ accounts while a stablecoin remains vulnerable through upgrade keys, minting authority, bridge attestations, or proof systems. Formal models should represent residual assumptions across layers rather than label one component “PQ-safe.” A

useful model must identify the controlling actor, inherited assumptions, value exposed, and state transition after another layer fails.

Gap: explicit authority and liability rules. Migration protocols should specify who declares an emergency, which checkpoint is authoritative, how users prove claims, how native and wrapped supply are reconciled, what happens after a deadline, how appeals and recovery work, and who absorbs losses from a late or failed migration. This analysis must combine cryptographic recovery with property, redemption, accounting, and liquidity consequences. Treating all participants as a single coordinated upgrader misses the central stablecoin problem.

Gap: bridge and wrapped-supply asymmetry. A destination representation depends on the source lockbox, attestation service, source finality, relayers, destination contract, exchanges, and liquidity venues. These components can migrate at different times. A technically secure new route does not extinguish claims or liquidity created by an old route. Research is needed on route versioning, authenticated checkpoints, redemption windows, legacy-route shutdown, detection of unbacked supply, and treatment of residual tokens after the old assumptions become unsafe.

Gap: dormant balances and coercive migration.. Leaving dormant balances untouched preserves current ownership rules but leaves a persistent quantum target. Freezing or recovering them reduces theft risk but changes control and may conflict with redemption, due-process, or customer-protection duties. The same governance dilemma has been identified for unmigrated cryptocurrency balances, with proposals ranging from leaving vulnerable assets spendable to freezing them after a deadline or introducing special recovery mechanisms [71]. Circle’s post-quantum roadmap gives the issuer’s side of this dilemma [18]. It separates disabling unsafe cryptographic control from extinguishing an asset holder’s economic interest, treats a post-cutoff freeze as a protective control rather than a finding of abandonment, and lists recovery routes: relocating frozen contracts to an issuer-controlled chain, zero-knowledge seed-recovery proofs for BIP-32 and SLIP-0010 hierarchies, TEE-attested seed verification, and off-chain evidence of entitlement. It identifies escheat and bailment as the closest legal analogues and asks regulators for guidance on notice periods, evidentiary standards, and recoverability windows. This contrasts with BIP-361’s rescue-protocol encumbrance [73] and Optimism’s announced January 2036 deadline as reported in the roadmap, neither of which specifies a recovery route. Stablecoin issuers thus have more administrative tools than base-layer protocols, but those tools make the governance choice more explicit rather than eliminating it. Migration mechanisms should state the trigger, notice period, proof of ownership, deadline, recovery route, and effect on redemption for users who do not or cannot act.

5.4 Privacy, Measurement, and Regulation Must Become Testable

Finding: private stablecoins use different cryptographic stacks. Private stablecoin designs do not share a single cryptographic stack. The Circle Research-Inco confidential ERC-20 design uses fully homomorphic encryption over encrypted balances and transfer

amounts, whereas note-based systems usually combine commitments, zero-knowledge proofs, nullifiers, viewing keys, and encrypted note data [43]. A third stack, planned for Circle’s Arc chain, executes standard contracts inside trusted execution environments with X-Wing HPKE transaction encryption and symmetric state encryption; its post-quantum privacy claim rests on enclave attestation and certificates that remain classical until the cloud provider upgrades them [18]. Each stack fails differently under a CRQC, and the residual dependency of the TEE design lies with a vendor outside the issuer’s control.

Gap: quantum-vulnerable supply measurement. Market capitalization alone obscures the distribution of risk among exposed user keys, issuer roles, bridge lockboxes, oracle committees, rollup proof systems, and private pools. We propose reporting *quantum-vulnerable supply* as a vector rather than one scalar:

$$QVS = (Q_{\text{user}}, Q_{\text{issuer}}, Q_{\text{bridge}}, Q_{\text{oracle}}, Q_{L2}, Q_{\text{privacy}}),$$

where each component measures stablecoin value whose continued integrity depends on a specified quantum-vulnerable assumption. Components should be reported per chain and representation, with explicit treatment of shared keys and overlapping dependencies to avoid double counting. Public tools should map contract roles, key exposure, bridge routes, oracle signer sets, rollup and proof dependencies, dormant balances, and migration status.

Gap: governance and regulatory readiness. Regulation increasingly requires reserve control, redemption, operational resilience, governance, and intervention capabilities, but post-quantum readiness is rarely expressed as a testable control. MiCA recovery and redemption duties imply that an issuer should demonstrate continued redemption under key loss, contract migration, or a freeze-and-reissue event [51]. The GENIUS Act and OCC proposals imply tests for preserving mint, burn, freeze, transfer-prevention, custody, screening, blocking, and reporting capabilities after a cryptographic transition [97, 98, 115]. Audits should therefore report both technical readiness and continuity of redemption, reserve control, legally required intervention, and historical evidence after classical signatures lose evidentiary value.

Research agenda. The strongest open problems are compositional. Future work should build stablecoin-specific benchmark suites, formal models of residual risk and authority, migration protocols for dormant and wrapped supply, efficient aggregate and threshold attestations for bridges and custody, PQ-friendly private and compliance-enabled transfers, and longitudinal measurements of quantum-vulnerable supply. The objective is an end-to-end transition that preserves authorization, redemption, supply integrity, finality, privacy, and required controls across every layer.

6 Conclusion

Stablecoins sit at the intersection of public blockchains, traditional finance, cross-chain infrastructure, and regulation. Their concentrated issuer, custody, oracle, bridge, and upgrade controls make them unusually sensitive to a CRQC, while their host-chain, rollup, and privacy dependencies prevent any one actor from completing the migration alone. The central stablecoin-specific problem is the authority–liability gap: the party able to change a component is

often different from the users, exchanges, protocols, or issuers that bear the loss if it fails.

A practical transition should begin with a function-level cryptographic inventory, protect issuer-controlled infrastructure, add contract, bridge, and oracle safeguards, adopt host-chain signature agility, and define explicit treatment of dormant and wrapped supply. Standardized KEMs and signatures provide necessary building blocks, but do not by themselves replace aggregate bridge attestations, threshold custody, private and compliance-enabled transfers, rolup proofs, or recovery governance. Regulation further constrains the result by requiring continuity of redemption, reserve control, audit evidence, and intervention capabilities.

The research agenda is therefore compositional. It includes complete-operation benchmarks, formal models of layered residual risk and migration authority, efficient aggregate and threshold authorization, post-quantum privacy and compliance mechanisms, protocols for dormant balances and legacy wrapped routes, and empirical measurement of quantum-vulnerable stablecoin supply. Progress should be measured not by whether one key has been replaced, but by whether authorization, redemption, supply integrity, finality, privacy, and legally required controls remain valid across the full stablecoin system.

References

- [1] Endre Abraham. 2018. Post-quantum verifiable random functions from ring signatures. Cryptology ePrint Archive, Report 2018/1231. <https://eprint.iacr.org/2018/1231>
- [2] Shweta Agrawal, Elena Kirshanova, Damien Stehlé, and Anshu Yadav. 2022. Practical, Round-Optimal Lattice-Based Blind Signatures. In *ACM CCS 2022*, Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi (Eds.). ACM Press, 39–53. doi:10.1145/3548606.3560650
- [3] Shweta Agrawal, Damien Stehlé, and Anshu Yadav. 2022. Round-Optimal Lattice-Based Threshold Signatures, Revisited. In *ICALP 2022 (LIPIcs, Vol. 229)*, Mikolaj Bojanczyk, Emanuela Merelli, and David P. Woodruff (Eds.). Schloss Dagstuhl, 8:1–8:20. doi:10.4230/LIPIcs.ICALP.2022.8
- [4] Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaiieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Jerome Lacan, Jean-Marc Robert, and Pascal Veron. 2022. *HQC*. Technical Report. National Institute of Standards and Technology. available at <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions>.
- [5] Md Mohaimin Al Barat, Shaoyu Li, Changlai Du, Y. Thomas Hou, and Wenjing Lou. 2024. SoK: Public Blockchain Sharding. arXiv preprint arXiv:2405.20521. <https://arxiv.org/abs/2405.20521>
- [6] Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan. 2022. Lattice-Based SNARKs: Publicly Verifiable, Preprocessing, and Recursively Composable - (Extended Abstract). In *CRYPTO 2022, Part II (LNCS, Vol. 13508)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, Cham, 102–132. doi:10.1007/978-3-031-15979-4_4
- [7] Algorand Foundation. 2026. Algorand Post-Quantum Cryptography Roadmap. Algorand Foundation technical blog. <https://algorand.co/blog/algorand-post-quantum-cryptography-roadmap>
- [8] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkatasubramanian. 2017. Liger: Lightweight Sublinear Arguments Without a Trusted Setup. In *ACM CCS 2017*, Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu (Eds.). ACM Press, 2087–2104. doi:10.1145/3133956.3134104
- [9] Thomas Attema, Vadim Lyubashevsky, and Gregor Seiler. 2020. Practical Product Proofs for Lattice Commitments. In *CRYPTO 2020, Part II (LNCS, Vol. 12171)*, Daniele Micciancio and Thomas Ristenpart (Eds.). Springer, Cham, 470–499. doi:10.1007/978-3-030-56880-1_17
- [10] Lukas Aumayr, Oguzhan Ersoy, Andreas Erwig, Sebastian Faust, Kristina Hostáková, Matteo Maffei, Pedro Moreno-Sanchez, and Siavash Riahi. 2021. Generalized Channels from Limited Blockchain Scripts and Adaptor Signatures. In *ASIACRYPT 2021, Part II (LNCS, Vol. 13091)*, Mehdi Tibouchi and Huaxiong Wang (Eds.). Springer, Cham, 635–664. doi:10.1007/978-3-030-92075-3_22
- [11] Ryan Babbush, Adam Zalcman, Craig Gidney, Michael Broughton, Tanuj Khattar, Hartmut Neven, Thiago Bergamaschi, Justin Drake, and Dan Boneh. 2026. Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations. PRX Quantum, accepted 6 July 2026. doi:10.1103/j3xf-bw18
- [12] Renas Bacho and Julian Loss. 2022. On the Adaptive Security of the Threshold BLS Signature Scheme. In *ACM CCS 2022*, Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi (Eds.). ACM Press, 193–207. doi:10.1145/3548606.3560656
- [13] Foteini Baldimtsi, Konstantinos Chalkias, and Arnab Roy. 2025. Post-Quantum Readiness in EdDSA Chains. Cryptology ePrint Archive, Report 2025/1368. <https://eprint.iacr.org/2025/1368>
- [14] Foteini Baldimtsi, Konstantinos Kryptos Chalkias, Yan Ji, Jonas Lindström, Deepak Maram, Ben Riva, Arnab Roy, Mahdi Sedaghat, and Joy Wang. 2024. zkLogin: Privacy-Preserving Blockchain Authentication with Existing Credentials. In *ACM CCS 2024*, Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie (Eds.). ACM Press, 3182–3196. doi:10.1145/3658644.3690356
- [15] Elaine Barker, Lily Chen, David Cooper, Dustin Moody, Andrew Regenscheid, Murugiah Souppaya, William Newhouse, Russ Housley, Sean Turner, William Barker, and Karen Kent. 2026. *Considerations for Achieving Crypto Agility: Strategies and Practices*. NIST Cybersecurity White Paper 39 Update 1. National Institute of Standards and Technology. doi:10.6028/NIST.CSWP.39-upd1
- [16] Yaser Baseri, Abdelhakim Hafid, Yahya Shahsavari, Dimitrios Makrakis, and Hassan Khodaiemehr. 2025. Blockchain Security Risk Assessment in Quantum Era, Migration Strategies and Proactive Defense. arXiv:2501.11798. doi:10.48550/arXiv.2501.11798
- [17] Hunter Beast, Ethan Heilman, and Isabel Foxen Duke. 2024. BIP-360: Pay-to-Merkle-Root (P2MR). Bitcoin Improvement Proposals. Draft; assigned 18 December 2024; version updated 29 July 2026. <https://github.com/bitcoin/bips/blob/master/bip-0360.mediawiki>
- [18] Mira Belenkiy, Duc V. Le, Gordon Liao, Vipin Singh Sehrawat, Dragos Rotaru, Sergey Gorbunov, Milap Sheth, Jay Logelin, Anthony De Abreu, and Dan Boneh. 2026. Circle's Post-Quantum Security Roadmap: Securing Blockchains, Smart Contracts, and Digital Assets for the Quantum Era. Circle technical roadmap. https://6778953.fs1.hubspotusercontent-na1.net/hubfs/6778953/PDFs/quantum_paper.pdf
- [19] Mihir Bellare, Ruth Ng, and Björn Tackmann. 2019. Nonces Are Noticed: AEAD Revisited. In *CRYPTO 2019, Part I (LNCS, Vol. 11692)*, Alexandra Boldyreva and Daniele Micciancio (Eds.). Springer, Cham, 235–265. doi:10.1007/978-3-030-26948-7_9
- [20] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. 2018. Scalable, transparent, and post-quantum secure computational integrity. Cryptology ePrint Archive, Report 2018/046. <https://eprint.iacr.org/2018/046>
- [21] Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nicholas Spooner, Madars Virza, and Nicholas P. Ward. 2019. Aurora: Transparent Succinct Arguments for R1CS. In *EUROCRYPT 2019, Part I (LNCS, Vol. 11476)*, Yuval Ishai and Vincent Rijmen (Eds.). Springer, Cham, 103–128. doi:10.1007/978-3-030-17653-2_4
- [22] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. 2012. High-speed high-security signatures. *Journal of Cryptographic Engineering* 2, 2 (Sept. 2012), 77–89. doi:10.1007/s13389-012-0027-1
- [23] Ward Beullens, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. 2023. Lattice-Based Blind Signatures: Short, Efficient, and Round-Optimal. In *ACM CCS 2023*, Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda (Eds.). ACM Press, 16–29. doi:10.1145/3576915.3616613
- [24] Alexander Bienstock, Leo de Castro, Daniel Escudero, Antigoni Polychroniadou, and Akira Takahashi. 2025. Efficient, Scalable Threshold ML-DSA Signatures: An MPC Approach. Cryptology ePrint Archive, Report 2025/1163. <https://eprint.iacr.org/2025/1163>
- [25] Blockstream Team. 2026. Blockstream Research Demonstrates Quantum-Resistant Transaction Signing on Liquid Using Simplicity Smart Contracts. Blockstream Research blog. <https://blog.blockstream.com/blockstream-research-demonstrates-quantum-resistant-transaction-signing-on-liquid-using-simplicity-smart-contracts/>
- [26] Dan Boneh, Justin Drake, Ben Fisch, and Ariel Gabizon. 2021. Halo Infinite: Proof-Carrying Data from Additive Polynomial Commitments. In *CRYPTO 2021, Part I (LNCS, Vol. 12825)*, Tal Malkin and Chris Peikert (Eds.). Springer, Cham, Virtual Event, 649–680. doi:10.1007/978-3-030-84242-0_23
- [27] Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham. 2003. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. In *EUROCRYPT 2003 (LNCS, Vol. 2656)*, Eli Bihem (Ed.). Springer, Berlin, Heidelberg, 416–432. doi:10.1007/3-540-39200-9_26
- [28] Dan Boneh, Ben Lynn, and Hovav Shacham. 2001. Short Signatures from the Weil Pairing. In *ASIACRYPT 2001 (LNCS, Vol. 2248)*, Colin Boyd (Ed.). Springer, Berlin, Heidelberg, 514–532. doi:10.1007/3-540-45682-1_30
- [29] Giacomo Borin, Sofia Celi, Rafaël del Pino, Thomas Espitau, Guilhem Niot, and Thomas Prest. 2025. Threshold Signatures Reloaded: ML-DSA and Enhanced Raccoon with Identifiable Aborts. Cryptology ePrint Archive, Report 2025/1166. <https://eprint.iacr.org/2025/1166>
- [30] Gilles Brassard, Peter Hoyer, and Alain Tapp. 1997. Quantum algorithm for the collision problem. arXiv preprint arXiv:quant-ph/9705002. <https://arxiv.org/abs/quant-ph/9705002>

- [31] Johannes A. Buchmann, Erik Dahmen, and Andreas Hülsing. 2011. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In *PQCrypto 2011*, Bo-Yin Yang (Ed.). Springer, Berlin, Heidelberg, 117–129. doi:10.1007/978-3-642-25405-5_8
- [32] Benedikt Bünz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh. 2020. Zether: Towards Privacy in a Smart Contract World. In *FC 2020 (LNCS, Vol. 12059)*, Joseph Bonneau and Nadia Heninger (Eds.). Springer, Cham, 423–443. doi:10.1007/978-3-030-51280-4_23
- [33] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. 2018. Bulletproofs: Short Proofs for Confidential Transactions and More. In *2018 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 315–334. doi:10.1109/SP.2018.00020
- [34] Maxime Buser, Rafael Dowsley, Muhammed Esgin, Clementine Gritti, Shabnam Kasra Kermanshahi, Veronika Kuchta, Jason Legrow, Joseph Liu, Raphael Phan, and Amin Sakzad. 2023. A Survey on Exotic Signatures for Post-Quantum Blockchain: Challenges and Research Directions. *Comput. Surveys* 55, 12 (2023), 1–32.
- [35] Maxime Buser, Rafael Dowsley, Muhammed F. Esgin, Shabnam Kasra Kermanshahi, Veronika Kuchta, Joseph K. Liu, Raphaël C.-W. Phan, and Zhenfei Zhang. 2022. Post-Quantum Verifiable Random Function from Symmetric Primitives in PoS Blockchain. In *ESORICS 2022, Part I (LNCS, Vol. 13554)*, Vijayalakshmi Atluri, Roberto Di Pietro, Christian Damsgaard Jensen, and Weihai Meng (Eds.). Springer, Cham, 25–45. doi:10.1007/978-3-031-17140-6_2
- [36] Vitalik Buterin, Eric Conner, John Dudley, Matthew Slipper, Ian Norden, and Abdelhamid Bakhta. 2019. EIP-2028: Transaction data gas cost reduction. Ethereum Improvement Proposals. <https://eips.ethereum.org/EIPS/eip-2028>
- [37] Rutchathon Chairattana-Apirom, Stefano Tessaro, and Chenzhi Zhu. 2024. Partially Non-interactive Two-Round Lattice-Based Threshold Signatures. In *ASIACRYPT 2024, Part IV (LNCS, Vol. 15487)*, Kai-Min Chung and Yu Sasaki (Eds.). Springer, Singapore, 268–302. doi:10.1007/978-981-96-0894-2_9
- [38] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. 2017. Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. In *ACM CCS 2017*, Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu (Eds.). ACM Press, 1825–1842. doi:10.1145/3133956.3133997
- [39] David Chaum. 1982. Blind Signatures for Untraceable Payments. In *CRYPTO'82*, David Chaum, Ronald L. Rivest, and Alan T. Sherman (Eds.). Plenum Press, New York, USA, 199–203. doi:10.1007/978-1-4757-0602-4_18
- [40] Circle Internet Financial. 2026. Stablecoin Smart Contracts on EVM-Compatible Blockchains. GitHub repository. Accessed 6 August 2026. <https://github.com/circlefin/stablecoin-evm>
- [41] Circle Internet Group. 2025. CCTP V1 Deprecation: CCTP V2 Is Now the Canonical CCTP. Circle blog. <https://www.circle.com/blog/cctp-version-updates>
- [42] Circle Internet Group. 2025. Introducing Circle xReserve: Enabling Interoperable USDC-Backed Stablecoins for Blockchains. Circle blog. <https://www.circle.com/blog/introducing-circle-xreserve>
- [43] Circle Research and Inco Network. 2024. Unveiling the Confidential ERC-20 Framework: Compliant Privacy on Public Blockchains Using FHE. Circle Research blog and whitepaper. <https://www.circle.com/blog/confidential-erc-20-framework-for-compliant-on-chain-privacy>
- [44] Coinbase. 2026. Coinbase Quantum Advisory Council Publishes Position Paper on Quantum Computing and Blockchain. Coinbase blog. <https://www.coinbase.com/blog/coinbase-quantum-advisory-council-publishes-position-paper-on-quantum-computing-and-blockchain>
- [45] David Cooper, Daniel Apon, Quynh Dang, Michael Davidson, Morris Dworkin, and Carl Miller. 2020. *Recommendation for Stateful Hash-Based Signature Schemes*. NIST Special Publication 800-208. National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-208
- [46] Renaud Dubois and Simon Masson. 2025. EIP-8051: Precompile for ML-DSA Signature Verification. Ethereum Improvement Proposals. Draft; created 15 October 2025. <https://eips.ethereum.org/EIPS/eip-8051>
- [47] Rachid El Bansarkhani and Jan Sturm. 2016. An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins. In *CANS 16 (LNCS, Vol. 10052)*, Sara Foresti and Giuseppe Persiano (Eds.). Springer, Cham, 140–155. doi:10.1007/978-3-319-48965-0_9
- [48] Muhammed F. Esgin, Oguzhan Ersoy, and Zekeriya Erkin. 2020. Post-Quantum Adaptor Signatures and Payment Channel Networks. In *ESORICS 2020, Part II (LNCS, Vol. 12309)*, Liqun Chen, Ninghui Li, Kaitai Liang, and Steve A. Schneider (Eds.). Springer, Cham, 378–397. doi:10.1007/978-3-030-59013-0_19
- [49] Muhammed F. Esgin, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu. 2019. Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications. In *CRYPTO 2019, Part I (LNCS, Vol. 11692)*, Alexandra Boldyreva and Daniele Micciancio (Eds.). Springer, Cham, 115–146. doi:10.1007/978-3-030-26948-7_5
- [50] Ethereum Foundation. 2026. Post-Quantum Ethereum. Ethereum research roadmap. Accessed 6 August 2026. <https://pq.ethereum.org/>
- [51] European Parliament and Council of the European Union. 2023. Regulation (EU) 2023/1114 on Markets in Crypto-Assets. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2023/1114>
- [52] Tiago M. Fernandez-Carames and Paula Fraga-Lamas. 2020. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* 8 (2020), 21091–21116.
- [53] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. 2019. PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. Cryptology ePrint Archive, Report 2019/953. <https://eprint.iacr.org/2019/953>
- [54] Shang Gao, Tianyu Zheng, Yu Guo, Zhe Peng, and Bin Xiao. 2025. Lattice-Based Zero-Knowledge Proofs for Blockchain Confidential Transactions. In *PKC 2025, Part V (LNCS, Vol. 15678)*, Tibor Jager and Jiaxin Pan (Eds.). Springer, Cham, 137–168. doi:10.1007/978-3-031-91832-2_5
- [55] Rosario Gennaro and Steven Goldfeder. 2018. Fast Multiparty Threshold ECDSA with Fast Trustless Setup. In *ACM CCS 2018*, David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang (Eds.). ACM Press, 1179–1194. doi:10.1145/3243734.3243859
- [56] Saurav Ghosh and Niloy Deb Roy Mishu. 2025. Quantum Blockchain Survey: Foundations, Trends, and Gaps. arXiv preprint arXiv:2507.13720. <https://arxiv.org/abs/2507.13720>
- [57] Jens Groth. 2016. On the Size of Pairing-Based Non-interactive Arguments. In *EUROCRYPT 2016, Part II (LNCS, Vol. 9666)*, Marc Fischlin and Jean-Sébastien Coron (Eds.). Springer, Berlin, Heidelberg, 305–326. doi:10.1007/978-3-662-49896-5_11
- [58] Lov K. Grover. 1996. A Fast Quantum Mechanical Algorithm for Database Search. In *28th ACM STOC*. ACM Press, 212–219. doi:10.1145/237814.237866
- [59] Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, and Arthur Gervais. 2020. SoK: Layer-2 Two Blockchain Protocols. In *FC 2020 (LNCS, Vol. 12059)*, Joseph Bonneau and Nadia Heninger (Eds.). Springer, Cham, 201–226. doi:10.1007/978-3-030-51280-4_12
- [60] Daira-Emma Hopwood and Jack Grigg. 2025. ZIP 2005: Orchard Quantum Recoverability. Zcash Improvement Proposals. Status: Proposed; Category: Consensus. <https://zips.z.cash/zip-2005>
- [61] Andreas Hülsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens. 2022. *SPHINCS**. Technical Report. National Institute of Standards and Technology. available at <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>
- [62] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. 2022. Transitioning organizations to post-quantum cryptography. *Nature* 605, 7909 (2022), 237–243.
- [63] Panos Kampanakis and Scott Fluhrer. 2017. LMS vs XMSS: A comparison of the Stateful Hash-Based Signature Proposed Standards. Cryptology ePrint Archive, Report 2017/349. <https://eprint.iacr.org/2017/349>
- [64] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. 2016. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In *CRYPTO 2016, Part II (LNCS, Vol. 9815)*, Matthew Robshaw and Jonathan Katz (Eds.). Springer, Berlin, Heidelberg, 207–237. doi:10.1007/978-3-662-53008-5_8
- [65] Emre Karabulut and Aydın Aysu. 2021. Falcon Down: Breaking Falcon Post-Quantum Signature Scheme through Side-Channel Attacks. Cryptology ePrint Archive, Report 2021/772. <https://eprint.iacr.org/2021/772>
- [66] Chelsea Komlo and Ian Goldberg. 2020. FROST: Flexible Round-Optimized Schnorr Threshold Signatures. In *SAC 2020 (LNCS, Vol. 12804)*, Orr Dunkelman, Michael J. Jacobson, Jr., and Colin O’Flynn (Eds.). Springer, Cham, 34–65. doi:10.1007/978-3-030-81652-0_2
- [67] Kris Kwiatkowski, Panos Kampanakis, Bas Westerbaan, and Douglas Stebila. 2026. *Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3*. Internet-Draft draft-ietf-tls-ecdhe-mlkem-05. Internet Engineering Task Force. Work in Progress, published 26 May 2026. <https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/>
- [68] Ruslan Kysil, István András Seres, Péter Kutas, and Nándor Kelecsényi. 2025. poqeth: Efficient, post-quantum signature verification on Ethereum. In *ASIACCS 25*. ACM Press, 327–343. doi:10.1145/3708821.3736193
- [69] Duc Viet Le, Mahimna Kelkar, and Aniket Kate. 2019. Flexible Signatures: Making Authentication Suitable for Real-Time Environments. In *ESORICS 2019, Part I (LNCS, Vol. 11735)*, Kazuo Sako, Steve Schneider, and Peter Y. A. Ryan (Eds.). Springer, Cham, 173–193. doi:10.1007/978-3-030-29959-0_9
- [70] Yuquan Li, Yuexin Xiang, Qin Wang, Tsz Hon Yuen, Andreas Deppeler, and Jiangshan Yu. 2026. SoK: Stablecoins in Retail Payments. arXiv:2601.00196. doi:10.48550/arXiv.2601.00196
- [71] Yehuda Lindell. 2026. Coinbase Quantum Advisory Council: Post-Quantum Migration and Abandoned Coins. Coinbase blog. <https://www.coinbase.com/blog/coinbase-quantum-advisory-council-post-quantum-migration-and-abandoned-coins>

- [72] Shengchen Ling, Yuefeng Du, Yajin Zhou, Lei Wu, Cong Wang, Xiaohua Jia, and Houmin Yan. 2025. SoK: Stablecoin Designs, Risks, and the Stablecoin LEGO. *arXiv:2506.17622*. doi:10.48550/arXiv.2506.17622
- [73] Jameson Lopp, Christian Papathanasiou, Ian Smith, Joe Ross, Steve Vaile, and Pierre-Luc Dallaire-Demers. 2026. BIP-361: Post Quantum Migration and Legacy Signature Sunset. Bitcoin Improvement Proposals. Draft; assigned 11 February 2026. <https://github.com/bitcoin/bips/blob/master/bip-0361.mediawiki>
- [74] Xingye Lu, Man Ho Au, and Zhenfei Zhang. 2019. Raptor: A Practical Lattice-Based (Linkable) Ring Signature. In *ACNS 2019 (LNCS, Vol. 11464)*, Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung (Eds.). Springer, Cham, 110–130. doi:10.1007/978-3-030-21568-2_6
- [75] Han Luo, Ziyi Yang, Jingquan Luo, Ziruo Wang, Yuexin Su, Xiaoming Sun, Lvzhou Li, and Tongyang Li. 2026. Quantum Algorithm for Elliptic Curve Discrete Logarithms with Space-Efficient Point Addition. *arXiv preprint arXiv:2607.13816*. doi:10.48550/arXiv.2607.13816
- [76] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai. 2022. *CRYSTALS-DILITHIUM*. Technical Report, National Institute of Standards and Technology. available at <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>.
- [77] Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Maxime Plançon. 2022. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. In *CRYPTO 2022, Part II (LNCS, Vol. 13508)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, Cham, 71–101. doi:10.1007/978-3-031-15979-4_3
- [78] Tushin Mallick, Maya Zeldin, Murat Cenk, and Cristina Nita-Rotaru. 2025. Quantum Disruption: An SoK of How Post-Quantum Attackers Reshape Blockchain Security and Performance. *arXiv:2512.13333*. doi:10.48550/arXiv.2512.13333
- [79] Gregory Markou and James Prestwich. 2026. EIP-8164: Native Key Delegation for EOAs. Ethereum Improvement Proposals. Draft; created 17 February 2026. <https://eips.ethereum.org/EIPS/eip-8164>
- [80] Patrick McCorry, Chris Buckland, Bennet Yee, and Dawn Song. 2021. SoK: Validating Bridges as a Scaling Solution for Blockchains. *Cryptology ePrint Archive*, Report 2021/1589. <https://eprint.iacr.org/2021/1589>
- [81] Ralph C. Merkle. 1988. A Digital Signature Based on a Conventional Encryption Function. In *CRYPTO'87 (LNCS, Vol. 293)*, Carl Pomerance (Ed.). Springer, Berlin, Heidelberg, 369–378. doi:10.1007/3-540-48184-2_32
- [82] Silvio Micali, Michael O. Rabin, and Salil P. Vadhan. 1999. Verifiable Random Functions. In *40th FOCS*. IEEE Computer Society Press, 120–130. doi:10.1109/SFCS.1999.814584
- [83] Silvio Micali, Leonid Reyzin, Georgios Vlachos, Riad S. Wahby, and Nickolai Zeldovich. 2021. Compact Certificates of Collective Knowledge. In *2021 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 626–641. doi:10.1109/SP40001.2021.00096
- [84] Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson, and David Cooper. 2024. *Transition to Post-Quantum Cryptography Standards*. NIST Internal Report 8547, Initial Public Draft. National Institute of Standards and Technology. doi:10.6028/NIST.IR.8547.ipd
- [85] Michele Mosca. 2018. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *Cryptology ePrint Archive*, Paper 2015/1075. <https://eprint.iacr.org/2015/1075>
- [86] Mysten Labs. 2025. Securing Sui in the Quantum Computing Era. Sui blog. <https://blog.sui.io/post-quantum-computing-cryptography-security/>
- [87] Ábel Nagy, János Tapolcai, István András Seres, and Bence Ladóczki. 2025. Forking the RANDAO: Manipulating Ethereum's Distributed Randomness Beacon. In *ACM CCS 2025*, Chun-Ying Huang, Jyh-Cheng Chen, Shih-Pyng Chen, David Lie, and Véronique Cortier (Eds.). ACM Press, 873–887. doi:10.1145/3719027.3744852
- [88] National Cybersecurity Center of Excellence and National Institute of Standards and Technology. 2023. Migration to Post-Quantum Cryptography: Quantum Readiness: Cryptographic Discovery. NIST SP 1800-38B Preliminary Draft. <https://www.nccoe.nist.gov/projects/migration-post-quantum-cryptography>
- [89] National Institute of Standards and Technology. 2024. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication 203. doi:10.6028/NIST.FIPS.203
- [90] National Institute of Standards and Technology. 2024. FIPS 204: Module-Lattice-Based Digital Signature Standard. Federal Information Processing Standards Publication 204. <https://csrc.nist.gov/pubs/fips/204/final>
- [91] National Institute of Standards and Technology. 2024. FIPS 205: Stateless Hash-Based Digital Signature Standard. Federal Information Processing Standards Publication 205. <https://csrc.nist.gov/pubs/fips/205/final>
- [92] National Institute of Standards and Technology. 2025. HQC Announced as a Fourth-Round Selection in the NIST PQC Standardization Process. NIST News. See NIST Internal Report 8545. <https://www.nist.gov/news-events/news/2025/03/nist-pqc-standardization-process-hqc-announced-4th-round-selection>
- [93] National Institute of Standards and Technology. 2026. Nine Candidates Advance to the Third Round of the Additional Digital Signatures for the PQC Standardization Process. NIST News. NIST Internal Report 8610. <https://www.nist.gov/news-events/news/2026/05/nine-candidates>
- advance-third-round-additional-digital-signatures-pqc
- [94] National Institute of Standards and Technology. 2026. Post-Quantum Cryptography Project. NIST Computer Security Resource Center. Accessed August 2026. <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>
- [95] Ngoc Khanh Nguyen and Gregor Seiler. 2022. Practical Sublinear Proofs for R1CS from Lattices. In *CRYPTO 2022, Part II (LNCS, Vol. 13508)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, Cham, 133–162. doi:10.1007/978-3-031-15979-4_5
- [96] Jakob Svennevik Notland, Jingyue Li, Mariusz Nowostawski, and Peter Halland Haro. 2024. SoK: Cross-Chain Bridging Architectural Design Flaws and Mitigations. *arXiv:2403.00405*. doi:10.48550/arXiv.2403.00405
- [97] Office of the Comptroller of the Currency. 2026. GENIUS Act: Anti-Money Laundering/Countering the Financing of Terrorism and Sanctions Compliance: Notice of Proposed Rulemaking. OCC Bulletin 2026-28. <https://www.occ.treas.gov/news-issuances/bulletins/2026/bulletin-2026-28.html>
- [98] Office of the Comptroller of the Currency. 2026. GENIUS Act Regulations: Notice of Proposed Rulemaking. OCC Bulletin 2026-3. <https://www.occ.treas.gov/news-issuances/bulletins/2026/bulletin-2026-3.html>
- [99] Christina Ovezik, Dimitris Karakostas, Mary Milad, Daniel W. Woods, and Angelos Kiayias. 2025. SoK: Measuring Blockchain Decentralization. In *ACNS 2025, Part I (LNCS, Vol. 15825)*, Marc Fischlin and Veelasla Moonsamy (Eds.). Springer, Cham, 184–214. doi:10.1007/978-3-031-95761-1_7
- [100] Torben P. Pedersen. 1992. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In *CRYPTO'91 (LNCS, Vol. 576)*, Joan Feigenbaum (Ed.). Springer, Berlin, Heidelberg, 129–140. doi:10.1007/3-540-46766-1_9
- [101] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. 2022. *FALCON*. Technical Report. National Institute of Standards and Technology. available at <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>.
- [102] Minfeng Qi, Qin Wang, Zhipeng Wang, Manvir Schneider, Tianqing Zhu, Shiping Chen, William Kottenbelt, and Thomas Hardjono. 2024. SoK: Bitcoin Layer Two (L2). *arXiv preprint arXiv:2409.02650*. <https://arxiv.org/abs/2409.02650>
- [103] Ronald L. Rivest, Adi Shamir, and Yael Tauman. 2001. How to Leak a Secret. In *ASIACRYPT 2001 (LNCS, Vol. 2248)*, Colin Boyd (Ed.). Springer, Berlin, Heidelberg, 552–565. doi:10.1007/3-540-45682-1_32
- [104] Claus-Peter Schnorr. 1991. Efficient Signature Generation by Smart Cards. *Journal of Cryptology* 4, 3 (Jan. 1991), 161–174. doi:10.1007/BF00196725
- [105] Peter W. Shor. 1994. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *35th FOCS*. IEEE Computer Society Press, 124–134. doi:10.1109/SFCS.1994.365700
- [106] Daniel R. Simon. 1997. On the Power of Quantum Computation. *SIAM J. Comput.* 26, 5 (1997), 1474–1483.
- [107] Nigel P. Smart. 2001. The Exact Security of ECIES in the Generic Group Model. In *8th IMA International Conference on Cryptography and Coding (LNCS, Vol. 2260)*, Bahram Honary (Ed.). Springer, Berlin, Heidelberg, 73–84. doi:10.1007/3-540-45325-3_8
- [108] Solana Foundation. 2026. Solana's Quantum Readiness. Solana Foundation. <https://solana.com/news/quantum-readiness>
- [109] Fatemeh Heidari Soureshjani, Mathias Hall-Andersen, MohammadMahdi Jahana, Jeffrey Kam, Jan Gorzny, and Mohsen Ahmadvand. 2023. Automated Analysis of Halo2 Circuits. *Cryptology ePrint Archive*, Report 2023/1051. <https://eprint.iacr.org/2023/1051>
- [110] StarkWare. 2026. The Architecture Advantage: Starknet's Post-Quantum Roadmap. StarkWare blog. <https://starkware.co/blog/the-architecture-advantage-starknets-quantum-readiness-roadmap/>
- [111] Hauke Malte Steffen, Georg Land, Lucie Johanna Kogelheide, and Tim Güneysu. 2023. Breaking and Protecting the Crystal: Side-Channel Analysis of Dilithium in Hardware. In *PQCrypto 2023*, Thomas Johansson and Daniel Smith-Tone (Eds.). Springer, Cham, 688–711. doi:10.1007/978-3-031-40003-2_25
- [112] Erkan Tairi, Pedro Moreno-Sanchez, and Matteo Maffei. 2021. Post-Quantum Adaptor Signature for Privacy-Preserving Off-Chain Payments. In *FC 2021, Part II (LNCS, Vol. 12675)*, Nikita Borisov and Claudia Diaz (Eds.). Springer, Berlin, Heidelberg, 131–150. doi:10.1007/978-3-662-64331-0_7
- [113] Wilson Abel Alberto Torres, Veronika Kuchta, Ron Steinfeld, Amin Sakzad, Joseph K. Liu, and Jacob Cheng. 2019. Lattice RingCT V2.0 with Multiple Input and Multiple Output Wallets. In *ACISP 19 (LNCS, Vol. 11547)*, Julian Jang-Jaccard and Fuchun Guo (Eds.). Springer, Cham, 156–175. doi:10.1007/978-3-030-21548-4_9
- [114] Wilson Abel Alberto Torres, Ron Steinfeld, Amin Sakzad, Joseph K. Liu, Veronika Kuchta, Nandita Bhattacharjee, Man Ho Au, and Jacob Cheng. 2018. Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0). In *ACISP 18 (LNCS, Vol. 10946)*, Willy Susilo and Guomin Yang (Eds.). Springer, Cham, 558–576. doi:10.1007/978-3-319-93638-3_32
- [115] United States Congress. 2025. Text of S. 1582: GENIUS Act. 119th Congress, Public Law 119-27. <https://www.congress.gov/bills/119th-congress/senate-bill/1582/text>

- [116] Gang Wang, Zhijie Jerry Shi, Mark Nixon, and Song Han. 2019. SoK: Sharding on Blockchain. Cryptology ePrint Archive, Report 2019/1178. <https://eprint.iacr.org/2019/1178>
- [117] Zhipeng Wang and Qianhong Wu. 2019. A Practical Lattice-Based Sequential Aggregate Signature. In *ProvSec 2019 (LNCS, Vol. 11821)*, Ron Steinfeld and Tsz Hon Yuen (Eds.). Springer, Cham, 94–109. doi:10.1007/978-3-030-31919-9_6
- [118] Gavin Wood. 2024. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper. Used for Ethereum precompile and gas-cost background. <https://ethereum.github.io/yellowpaper/paper.pdf>
- [119] Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto Di Pietro, and Aiman Erbad. 2024. A Survey and Comparison of Post-Quantum and Quantum Blockchains. arXiv:2409.01358. doi:10.48550/arXiv.2409.01358
- [120] Luyao Zhang. 2025. SoK: Stablecoins for Digital Transformation – Design, Metrics, and Application with Real World Asset Tokenization as a Case Study. arXiv:2508.02403. doi:10.48550/arXiv.2508.02403
- [121] Luyao Zhang, Xinshi Ma, and Yulin Liu. 2022. SoK: Blockchain Decentralization. arXiv preprint arXiv:2205.04256. <https://arxiv.org/abs/2205.04256>
- [122] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. 2023. SoK: Decentralized Finance (DeFi) Attacks. In *2023 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 2444–2461. doi:10.1109/SP46215.2023.10179435

A Supplementary Cryptographic Details

This appendix provides formal definitions for Section 2.

Hash functions. A hash function family $H : \mathcal{K} \times \mathcal{M} \rightarrow 0, 1^\lambda$ maps an arbitrary-length message to a fixed-length digest.

PROPERTY 1 (HASH SECURITY). A hash function should satisfy **preimage resistance** (given $y = H(m)$, find m' with $H(m') = y$), **second-preimage resistance** (given m , find $m' \neq m$ with $H(m') = H(m)$), and **collision resistance** (find any $m \neq m'$ with $H(m) = H(m')$).

Quantum impact. Grover [58] gives a quadratic preimage speedup ($\Theta(2^{\lambda/2})$), and BHT [30] gives $\Theta(2^{\lambda/3})$ for collisions assuming quantum RAM; under the realistic parallel/low-memory model the classical $2^{\lambda/2}$ collision bound dominates. Grover parallelizes poorly (a $\sqrt{k}$ speedup over k instances), so 256-bit hashes (SHA-256, SHA3-256, Keccak-256, BLAKE2b/3) retain ≈ 128 -bit post-quantum security.

Post-quantum stance. No change of primitive is required; use 256-bit outputs everywhere Merkle roots, nullifiers, or commitments must remain unforgeable. Hash-based signatures (SLH-DSA, XMSS, LMS) and STARK proof systems [20, 31, 61, 63] inherit post-quantum (PQ) security entirely from these properties.

Digital signatures. A signature scheme $\Sigma = (\text{KeyGen}, \text{Sign}, \text{Verify})$ is required to satisfy **existential unforgeability under chosen-message attack** (EUF-CMA): no PPT adversary with signing-oracle access can produce a valid signature on a fresh message except with negligible probability.

Quantum impact. Every blockchain-deployed scheme based on DLP/IFP (ECDSA, Schnorr [104], EdDSA [22], RSA-PSS, BLS [28]) falls to Shor [105]: sk is recovered from pk without any oracle access, so EUF-CMA is broken outright. Crucially, **non-repudiation is broken retroactively**; a forgery produced after a CRQC is cryptographically indistinguishable from an honest historical signature, undermining audit logs, reserve attestations, and legal evidence. The Google Quantum AI estimate [11] distinguishes the *at-rest* regime (pk already on chain) from the *on-spend* regime (pk revealed at spending time); issuer, treasury, bridge, and oracle keys are almost always at-rest.

Post-quantum candidates. NIST has standardized ML-DSA and SLH-DSA and is continuing standardization of FN-DSA, based on Falcon: ML-DSA(FIPS 204 [90], derived from Dilithium [76]), lattice-based, ≈ 1.3 – 2.6 KB public keys and 2.4 – 4.6 KB signatures, the default for issuer admin and oracle workloads; SLH-DSA(FIPS 205 [91], derived from SPHINCS+), stateless hash-based with 8 – 49 KB signatures, attractive for cold-path treasury actions; and Falcon [101], NTRU lattice, compact (≈ 666 B) but with side-channel-sensitive Gaussian sampling. Code- (CROSS, LESS), multivariate- (UOV, MAYO), and isogeny-based (SQIsign) families are less mature. Critically, **none support non-interactive aggregation** comparable to BLS, creating an important limitation for bridge committees.

Multi-signatures and threshold signatures. A (t, n) -threshold signature scheme distributes signing across n parties so that any $\geq t$ can jointly sign and fewer than t corruptions cannot, with additional desiderata of **robustness** and **identifiable abort**. Threshold ECDSA, threshold Schnorr (FROST), and threshold BLS [12, 28, 55, 66] all reduce to DLP/pairing assumptions; under Shor, the aggregate sk is recovered directly from the aggregate pk , so the threshold policy provides no protection whatsoever: a quantum-empowered single adversary acts as if all n shares were compromised. This is severe because most institutional custody, exchange hot wallets, and bridge committees deploy a threshold or multi-sig over a DL-based scheme. Lattice-based multi- and threshold-signature constructions exist [3, 37, 47], but production gaps remain in dynamic committees, identifiable abort, HSM/MPC integration, and aggregate sizes within current calldata budgets.

Key exchange and authenticated channels. A KEM (KeyGen, Encaps, Decaps) is **IND-CCA secure** if no PPT adversary can distinguish a real encapsulated key from uniform even with decryption oracle access. Classical DH/ECDH, ECIES [107], and RSA-OAEP all reduce to DLP or factoring and lose IND-CCA security under Shor. The dominant pattern is **store-now-decrypt-later** (SNDL): adversaries archive encrypted issuer-custodian traffic today and decrypt it once a CRQC exists, exposing signing-ceremony schedules, reserve instructions, compliance correspondence, and bridge relayer topology. ML-KEM is standardized in FIPS 203 [89]; HQC [4] has been selected for standardization as a backup KEM. Production deployments use **hybrid KEMs** (e.g., X25519+ML-KEM-768 in TLS 1.3) that remain secure as long as either component does, giving a clean transition story for issuer APIs and custodian links.

Randomness, VRFs, and leader election. A verifiable random function (VRF) is (KeyGen, Eval, Verify) where $\text{Eval}_{sk}(x) \rightarrow (y, \pi)$.

PROPERTY 2 (VRF SECURITY). A VRF satisfies **uniqueness** (at most one y verifies for given pk, x), **pseudorandomness** (y is indistinguishable from uniform without sk , even given proofs on other inputs), and **public verifiability**.

Quantum impact. Deployed EC-VRFs (Algorand, Cardano/Chainlink) base both uniqueness and pseudorandomness on DLP; under Shor, sk is recovered, **pseudorandomness is fully lost** (all future outputs become predictable), and **uniqueness may also fail** depending on construction. Threshold-BLS beacons (drand) are broken at the threshold level, allowing biased or fully-controlled

beacon outputs. For stablecoins this affects PoS validator/committee selection, liquidation auctions, and any governance lottery.

Post-quantum candidates. Symmetric-primitive VRFs [35] reduce pseudorandomness to hash/PRP assumptions at the cost of large (tens of KB) proofs; ring-signature-based PQ VRFs [1] achieve both properties from lattice assumptions. Every current PQ VRF is substantially slower or larger than ECVRF, and integration with light-client committee sampling remains unsolved.

A.0.1 Cryptography for Privacy and Advanced Functionality.

Zero-knowledge proofs. A non-interactive zero-knowledge (NIZK) argument for NP-relation $\mathcal{R}$ is (Setup, Prove, Verify).

PROPERTY 3 (NIZK SECURITY). A NIZK satisfies **completeness** (honest proofs verify), **(knowledge) soundness** (no efficient prover convinces Verify of $x \notin \mathcal{L}_{\mathcal{R}}$; the knowledge variant requires an extractor recovering w), and **zero-knowledge** (a simulator produces proofs indistinguishable from real ones without w).

Quantum impact. Quantum attacks affect different properties of different systems: Groth16 [57], PLONK [53] with KZG, Bulletproofs [33], and Halo/Halo2 [26, 109] all derive (knowledge) soundness from pairing or DLP assumptions, and Shor breaks soundness in each case, enabling accepting proofs for false statements (e.g., unbacked rollup state transitions or shielded notes minted from nothing). STARKs [20] rely only on hash collision resistance and FRI low-degree testing, so their soundness degrades only marginally under Grover and they are treated as PQ-secure today. Note that *zero-knowledge* typically survives quantum adversaries given a uniform random tape, but Fiat–Shamir constructions require re-analysis in the QROM via measure-and-reprogram or online-extraction techniques.

Post-quantum candidates. STARKs / hash-based IOPs [20] offer transparent setup and PQ soundness at the cost of larger (~ 50 – 200 KB) proofs amortizable via recursion. Lattice-based SNARKs provide publicly verifiable, preprocessing, recursive constructions [6] and sublinear R1CS arguments [77, 95]; lattice ZK is also tuned for the range and equality proofs needed for confidential stablecoin transfers [49, 54]. MPC-in-the-head systems (Ligero, Aurora, Picnic) [8, 21, 38] yield proofs from symmetric primitives at larger sizes but minimal assumptions.

Commitment schemes. (Com, Open) binds a committer to m without revealing it.

PROPERTY 4 (COMMITMENT SECURITY). A commitment is **hiding** (commitments to m_0, m_1 are indistinguishable) and **binding** (no efficient $\mathcal{A}$ opens the same commitment to two distinct values). Each property may be computational or statistical; the two cannot both be statistical.

Quantum impact. **Pedersen commitments** [100] are statistically hiding and computationally binding under DLP; *binding falls to Shor*, letting an adversary equivocate a single commitment to multiple values: forging proof-of-reserves or double-spending confidential transfers in Monero, MumbleWimble, Zether [32], and bulletproof-based systems. The statistical hiding property survives. **Hash-based commitments** $c = H(m \parallel r)$ are computationally hiding and statistically binding in the random-oracle model; binding

degrades to $\approx 2^{\lambda/2}$ under Grover (acceptable for $\lambda = 256$), and hiding remains comfortable when $|r| \geq 256$ bits. **KZG/polynomial commitments** are binding under q -SDH/pairing assumptions and broken by Shor, affecting PLONK-style proofs and Ethereum EIP-4844 blobs.

Post-quantum candidates. Hash-based commitments are a natural drop-in for nullifier and note commitments in Zcash/Aztec-style pools. Lattice-based SIS commitments [9] are homomorphic and integrate with lattice ZK proofs of opened-value arithmetic. Code-based commitments from LPN exist but are uncommon in production stacks.

Encryption and AEAD. Symmetric AEAD targets indistinguishability under chosen-ciphertext attack and integrity of ciphertext. Symmetric ciphers face Grover-style brute-force key search: AES-128 retains only ≈ 64 -bit quantum security in a strong query model and AES-256 retains ≈ 128 , motivating 256-bit keys post-quantum. Under *superposition queries* to a keyed primitive (an unrealistic model for blockchain settings but consequential for standardization), Kaplan et al. [64] showed Simon’s algorithm breaks several MAC and mode constructions including CBC-MAC in polynomial time.

B Cost Evidence and Benchmarking Details

Cost figures are meaningful only together with their execution model. Table 9 separates deployed precompiles, calldata-only calculations, draft protocol costs, and measured ordinary-EVM verification. The EIP figures are proposals, not deployed Ethereum prices. The *poqeth* values are measured gas costs for specific schemes and NIST-level-1 parameter choices [68].

Stablecoin benchmark scenarios. A stablecoin benchmark should evaluate complete operations: mint or burn authorization; threshold custody withdrawal; bridge attestation and redemption; oracle update and retry; user or dormant-balance migration claims; private transfer and selective disclosure; and rollup settlement. Each benchmark should report bytes, gas or native verifier cost, data-availability overhead, signer throughput, end-to-end latency, HSM/MPC support, wallet memory, audit evidence, and behavior under signer or relayer failure.

Mechanism	Key/signature	Verification/data cost	Evidence type	Stablecoin interpretation
ECDSA/secp256k1	65-byte signature	3,000 gas for ecrecover; about 1,040 calldata gas	Deployed precompile and calldata schedule [36, 118]	Current account and administrator baseline
ML-DSA-44 calldata	1,312-byte public key; 2,420-byte signature	About 38,720 calldata gas for non-zero signature bytes	Calculation from FIPS 204 and EIP-2028 [36, 90]	Excludes verification, public-key storage, aggregation, and transaction overhead
EIP-8051	20,512-byte expanded verifier key; 2,420-byte signature	4,500 gas proposed	Draft specialized precompile [46]	Low price depends on protocol support and expanded key representation
EIP-8164	1,312-byte key; 2,420-byte signature	50,000 intrinsic gas proposed	Draft native account rule [79]	Includes an account migration mechanism but not contract, bridge, or validator migration
<i>poqeth</i> W-OTS+	Parameter-specific	222,114 on-chain; 126,095 Naysayer gas	Measured EVM implementation [68]	Optimistic verification lowers cost but adds dispute and trust assumptions
<i>poqeth</i> XMSS	Parameter-specific	4,363,623 on-chain; 594,572 Naysayer gas	Measured EVM implementation [68]	Stateful signing can be managed off-chain, but verification remains expensive
<i>poqeth</i> SPHINCS+	Parameter-specific	11,617,690 on-chain; 693,721 Naysayer gas	Measured EVM implementation [68]	Conservative hash assumptions do not imply cheap contract verification
<i>poqeth</i> MAYO	Parameter-specific	938,752,492 on-chain; 107,634,064 Naysayer gas	Measured EVM implementation [68]	Compact signatures can still require prohibitive verifier arithmetic
SLH-DSA	Parameter-dependent; signatures in the kilobyte-to-tens-of-kilobytes range	Workload and implementation dependent	NIST standard [91]	Plausible for cold recovery, generally unsuitable for frequent L1 messages without aggregation

Table 9: Representative post-quantum verification and data costs. Values are not directly comparable across execution models.