The MetaMUI Blue Paper

Quantum-Safe Identity-Based Settlement Infrastructure

Phantom Seokgu Yun · Architect and Founder
Frances Kim, Ph.D. · Head of Research and Co-Founder

Verify, don't trust.

Mainnet Hard Fork Edition · September 2026

MetaMUI

Quantum-Safe Identity-Based Settlement Infrastructure

Phantom Seokgu Yun
Architect and Founder

Frances Kim, Ph.D.
Head of Research and Co-Founder

This Blue Paper describes the architecture, cryptographic design, migration model, consensus, cross-chain security, integration model, deployment status, and known limitations of the MetaMUI mainnet following the hard fork completed on 13 September 2026 at block 35,499,408.

Verify, don't trust.

EVERY CLAIM IN THIS PAPER NAMES WHERE IT CAN BE CHECKED

CONTENTS

Part 0 Executive Summary

As of 13 September 2026, MetaMUI operates on its post-quantum mainnet architecture, following a completed hard fork. Every technical statement in this paper describes that network as it now runs. Where the previous architecture is relevant, it is named as such.

Most major blockchains now have a quantum roadmap. As Reuters reported in July 2026, none of the top 20 blockchains had implemented a post-quantum signature algorithm, according to people interviewed for that story. Our own survey, with sources and dates, is Appendix B.

That gap is not a failure of will. It is architectural. Chains built on the assumption that an address is a public key cannot adopt post-quantum cryptography without asking every holder to move their assets by hand. A co-author of Bitcoin's own post-quantum proposal estimates seven years for that transition, and adds: *"I'm just spitballing here. No one actually knows."* Google's researchers place cryptographically relevant quantum computing at 2029. The optimistic estimate finishes four years after the threat window is estimated to open.

MetaMUI did not retrofit. Its mainnet has been identity-based since 2021 — an account is a decentralized identifier, and a key is a credential registered against it — and the hard fork rebuilt cryptography, identity, and ledger as one system on that foundation. Identity is not an application layer here. It is the primitive.

The consequence is the part no chain in our survey has solved: users do not move their assets to become quantum-safe. Nothing moves at all.

Five questions, and where MetaMUI stands

1 **Is it live on mainnet, or a demonstration?** LIVE

Live. The hard fork is complete and the network is in production. explorer.metamui.id

2 Is it complete across the stack, or only the signature layer?

SIGNING · IDENTITY · CONSENSUS

Post-quantum signatures cover transaction signing, identity, and consensus (§2.5, §2.6). Two qualifications belong here rather than in a footnote. Proof-of-work chains have no consensus signatures to protect, so several post-quantum proof-of-work chains clear this bar today, and they clear it honestly. And among chains whose consensus does use signatures, MetaMUI's position rests on a design choice rather than a cryptographic result: a permissioned-public validator set has no randomized leader election to protect. **MetaMUI has not solved the quantum-safe VRF problem; the architecture does not encounter it.**

3 Is it fast enough to actually use? P50 ≈ 65 MS

MetaMUI signs with Falcon-512, selected because compact signatures keep verification cost low — the requirement for payment infrastructure, which verifies far more often than it signs (§2.5). Falcon is being standardized as FN-DSA under NIST FIPS 206, still at draft stage; we say so rather than imply a final standard. Finality is deterministic and reached in a single block: once a majority of registered validators have signed their finality votes, the block is irreversible. Measured from transaction submission to irreversibility, median finality is approximately 65 ms, with a 99th percentile of approximately 524 ms — on a three-validator set in a single region. Appendix A states the configuration in full, and is explicit about what that figure does and does not establish.

4 Does it migrate without moving assets? IN PLACE

Yes — and this is the bar, stated precisely. Chains built post-quantum from genesis, QRL among them, never had a classical user base to migrate. Among chains that do have one: Bitcoin's holders must spend to a new output type by hand, and Algorand — whose native Falcon-1024 accounts went live on mainnet in August 2026 — issues them as separate, opt-in accounts that holders create and fund themselves. Ethereum, the XRP Ledger, and Polkadot have each designed an in-place upgrade — none is live. Appendix B.2 gives the detail with sources.

MetaMUI had a classical user base on its mainnet and moved it in place. **Migration is a key registration, not an asset migration** (§2.4).

5 **Is it secure in motion, not just at rest?** DUAL SIGNATURE · KEYLESS

Bridges are the most exploited category in the industry, and the largest losses came from stolen signing keys rather than defective code. MetaMUI requires two independent cryptographic systems to clear a transfer on the classic-chain side, and runs approval through a keyless protocol account with no master key on the MetaMUI side (§2.9).

Verify, don't trust

The mainnet explorer is public. The post-quantum implementations, the Wallet SDK, and the blockchain core — including consensus and the DID structure — are published for review under the Business Source License, so the cryptography described here can be read rather than taken on our word. A demo network for hands-on testing opens in September 2026 and will be available to institutions and other chains on request.

→ explorer.metamui.id → github.com/SovereignWallet-Network

Demo network — opening September 2026 → Appendix A

We document what is running. Where something is in progress, this paper says so — see Part 5.

Part 1 Why Existing Blockchains Cannot Simply Migrate

Nothing in this part is a prediction, and none of the numbers in it are ours. They come from the standards body setting the deadline, from the researchers estimating the threat, and from the engineers doing the migration work on the chains that have started it. Where those sources disagree, we say so. Where they admit they are guessing, we quote the admission.

1.1 The two clocks

The first clock is the threat. Google's researchers place the arrival of quantum computers capable of breaking current encryption at around 2029, an estimate that has moved earlier rather than later as resource requirements have been revised down. NIST's transition roadmap does not wait for that date to settle: its draft schedule deprecates ECDSA and RSA at the 112-bit security level after 2030 and disallows them after 2035; the higher security levels are disallowed on the same date. For any institution following federal cryptographic guidance, elliptic-curve signatures have an expiry date on the calendar regardless of what a quantum computer achieves.

Nobody knows the threat date. That is the point rather than an objection to it: a deadline you cannot predict is only manageable if the work it requires is short. This work is not short.

The second clock is the transition. A co-author of Bitcoin's post-quantum proposal has published the only detailed public estimate we are aware of, and it is worth reading in full rather than in summary: two and a half years to write the proposals and get the code reviewed and tested, half a year to activate — "assuming everyone wants it" — and then, "if we are lucky, 90% will have updated five years after activation." Seven years in total. He adds: *"I'm just spitballing here. No one actually knows."*

We quote the caveat because it belongs to the estimate. It also cuts one way rather than both: the seven years assume consensus that does not yet exist, and an update rate the ecosystem has never achieved.

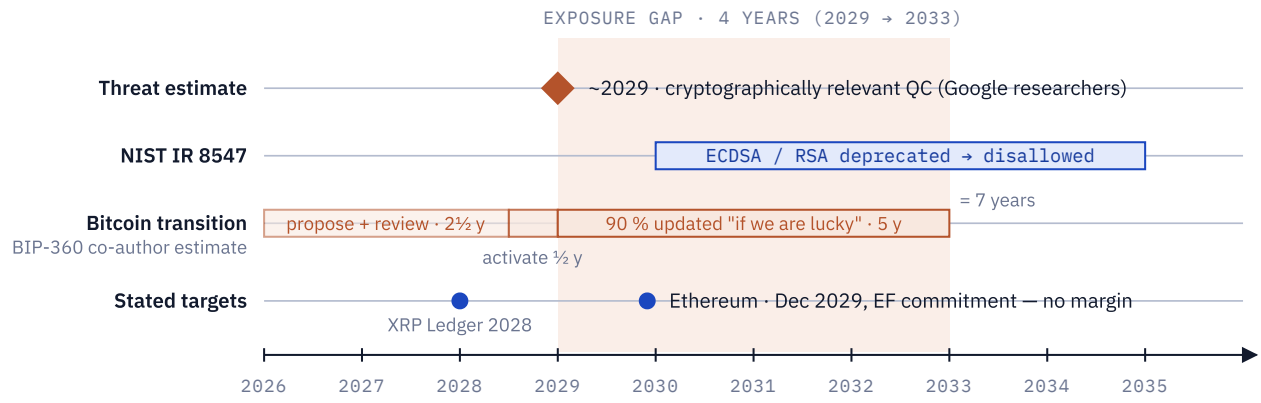

FIGURE 1 The two clocks. The most optimistic published transition estimate for Bitcoin ends in 2033; the threat estimate is 2029. The shaded band is the four years in which a manual migration is still under way after the threat window is estimated to open. Sources: Appendix D, refs. 1–3.

The arithmetic is not close. Seven years from 2026 ends in 2033. The threat estimate is 2029; the regulatory disallow date is 2035. The most optimistic published figure, offered from inside the chain with the most at stake, finishes four years after the threat window opens.

In September 2026 the Ethereum Foundation committed to full quantum resistance — execution, consensus and data — by December 2029, and published the fork sequence to get there: a scoping upgrade in late 2026 carrying no post-quantum work, a public-key registry around mid-2028, a "minimum viable" post-quantum release in late 2028, and post-quantum attestations in December 2029. The Foundation describes that deadline as non-negotiable at least until it reassesses quantum progress in January 2027.

We cite it because it is the most concrete published schedule in the industry, and because of what it concedes on its own terms: more than three years of sequenced protocol work, on the chain with the largest engineering capacity, arriving in the same year the threat is estimated to. There is no margin in it.

And as of July 2026, according to people interviewed by Reuters, none of the top 20 blockchains had implemented a post-quantum signature algorithm at all. Appendix B sets out where each stands, with sources and dates, so a reader can check what has moved since.

These are not chains that failed to notice. They are chains that started too late for an architecture that makes the work this large.

1.2 Why retrofitting fails

Three costs compound, and each is enough to slow a migration on its own.

Signatures get bigger, and the cost multiplies through the system. In BNB Chain's published evaluation of ML-DSA-44, signatures grew from 65 to 2,420 bytes — roughly thirty-seven times — a native transfer from about 110 bytes to 2.5 KB, blocks from about 130 KB to 2 MB, and cross-region native-transfer throughput fell from roughly 4,970 to 3,000 transactions per second, with gas throughput halved. Larger signatures mean fewer transactions per block, more bandwidth between nodes, and more verification work on every machine in the network — three effects that multiply rather than add. A chain can absorb this. A payment network being asked to settle at scale absorbs it as a permanent tax.

BNB CHAIN EVALUATION · ML-DSA-44	CLASSICAL	POST-QUANTUM	CHANGE
Signature size	65 B	2,420 B	× 37
Native transfer	~110 B	~2.5 KB	× 23
Block size	~130 KB	~2 MB	× 15
Cross-region transfer throughput	4,973 TPS	2,997 TPS	– 40 %
Gas throughput	—	—	halved

An engineering assessment, not a mainnet or public-testnet deployment. Appendix D, ref. 4.

The chain is the smallest part of the change. Wallets, hardware wallets, custodians, exchanges, HSMs, key ceremonies, bridges, explorers, indexers, accounting systems, and every integration built against the old signature format have to change too, in a coordinated sequence, without breaking the systems they connect. One senior cybersecurity executive interviewed by Reuters expected two years for their own company alone to reach full quantum resistance. The comparison drawn in that reporting is Y2K, which cost more than $300 billion globally — and Y2K had a fixed, known date and no adversary with an incentive to arrive early.

And then governance has to decide something it would rather not. Once a post-quantum address format exists, a chain must answer a question with no comfortable answer: what happens to the coins that never move? Leaving them is leaving a growing pool of publicly visible, provably vulnerable value on the ledger — on Bitcoin, a draft sunset proposal records that more than a third of all bitcoin sit at addresses whose public keys have already been revealed on-chain. Freezing them means confiscating property from holders who did nothing wrong, on a network whose central promise is that this cannot happen. Both answers cost the chain something it advertises about itself. Bitcoin, five years after Taproot activated, is by one account "still having a civil war over the downstream effects" of that upgrade — and Taproot did not ask anyone to move a coin.

1.3 The unsolved variable: users

Every migration plan for every existing chain ends at the same step, and it is always the last one: **each holder must move their assets, by hand, to a new address.**

This is where security stops being a property of the protocol and becomes a property of human behavior. The estimate above is explicit: if we are lucky, 90% five years after activation. The remaining tenth is not a rounding error. On a public ledger it is a visible, addressable, permanently listed set of accounts holding real value under cryptography known to be broken, and it includes exactly the holders least able to act — lost keys, inactive accounts, estates, and the coins of people who are no longer alive.

The asymmetry is the problem. A migration is a success at 90%; an attacker does not need it to fail. They need the stragglers, and the ledger tells them precisely where the stragglers are.

There is also a window rather than a moment. Throughout a manual migration, every holder is being asked to send their entire balance to a new address they have never used before, on the instruction of software they are told to trust — structurally, the exact scenario every phishing campaign has ever tried to manufacture. The migration does not merely fail to protect the users who don't act. It creates a period of maximum exposure for the ones who do.

> *"Safe, if everyone acts" is not a security property. It is a hope with a deadline attached, and the deadline is set by someone else.*

The question this raises is narrow, and Part 2 is the answer to it: **what would a chain have to look like for migration not to require its users to act at all?**

Part 2 MetaMUI Architecture

This part describes the network as it now runs. Each section states what the architecture is and why it is built that way; where a design decision has a cost, the cost is stated with it.

2.0 What the hard fork changed

MetaMUI's mainnet has been identity-based since 2021. That property was not adopted for quantum reasons — it was chosen for regulated finance and central bank work, where an account must be attributable to a verified party — and it is the reason the hard fork was possible at all. The table below is therefore as notable for its unchanged rows as for its changed ones.

PROPERTY	PREVIOUS ARCHITECTURE (2021 – 2026)	CURRENT MAINNET (AS OF 13 SEPTEMBER 2026)
Account model	DID — identifier is the account	Unchanged
Identity data on ledger	None; held by Identity Verifier	Unchanged
Ledger scope	Identifiers, key bindings, balances, governance	Unchanged
Signature verification	Single algorithm	**Multi-algorithm, concurrent**
User transaction signatures	Sr25519	**Falcon-512**
Consensus signatures	Classical	**Falcon-512 finality votes**
Keys per identifier	One	**Several, of different algorithms**
Key rotation	Within one algorithm	**Across algorithms**
Identifier namespace	`did:ssid:`	**`did:mmui:`** — migrated automatically
Cross-chain transfer authorization	—	**Dual signature + keyless protocol account**
Offline payment	Demonstrated 2023	Not on mainnet — see Part 5

Why this had to be a hard fork. The 2021 runtime verified one signature scheme. Every signature it accepted — those users produce to authorize transactions, and those validators exchange to agree on a block — was classical, and the verification path assumed as much. Post-quantum operation requires the opposite property: the verifier must accept several algorithms at once, classical and post-quantum together, on both paths.

That cannot ship as an optional upgrade. A node running the earlier code cannot verify a Falcon-signed block; presented with a valid chain, it rejects it. Changing what the verifier accepts is a consensus-breaking change by definition, and a consensus-breaking change is a hard fork. There was no version of this work releasable as a wallet feature, a runtime module, or an opt-in.

2.1 System architecture

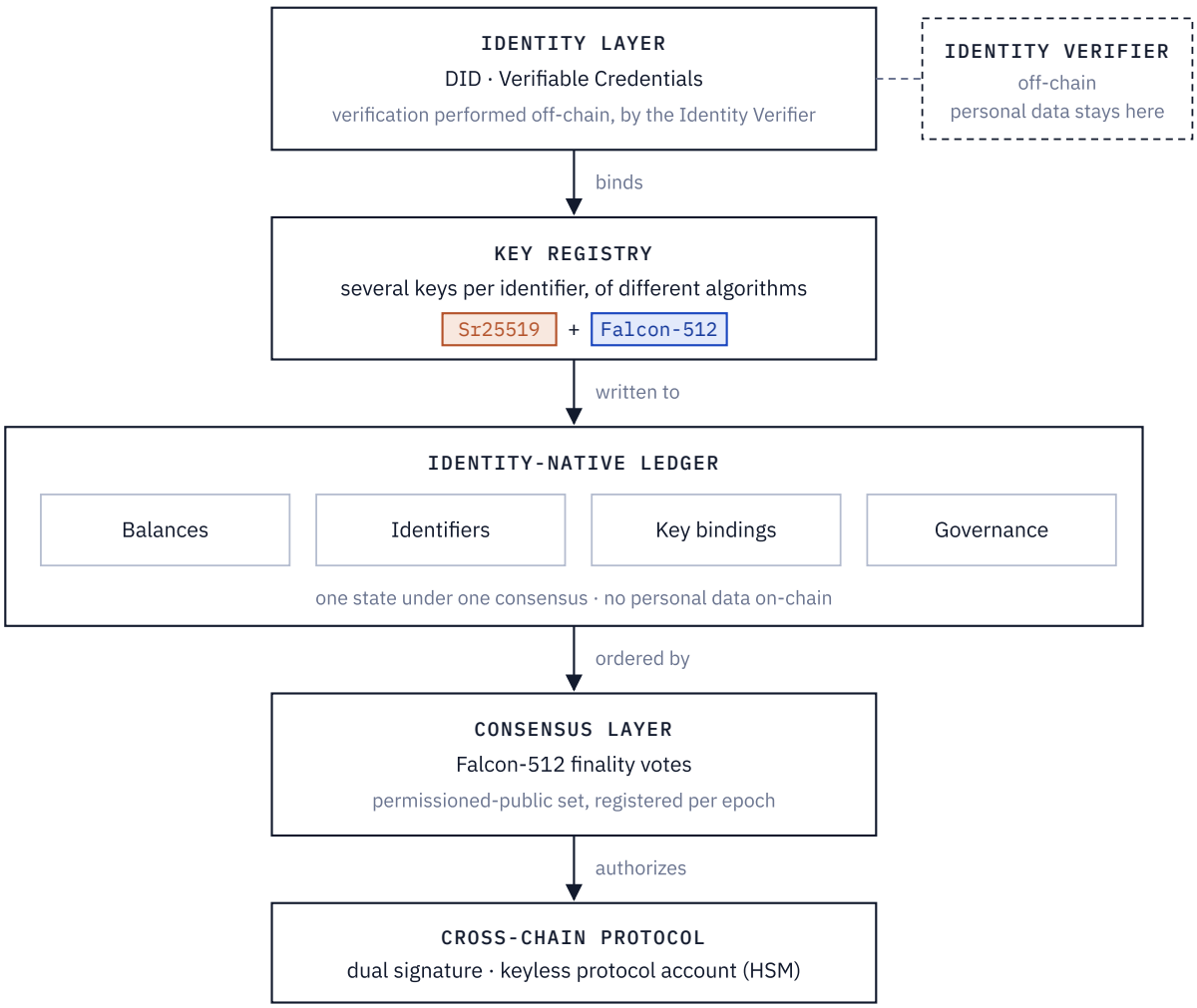

FIGURE 2 The MetaMUI stack. Identity sits above the key registry, not beside it; everything below the identity layer is the identity-native ledger, one state under one consensus. Personal data stops at the Identity Verifier and never reaches the chain.

Two things about this stack are worth reading off the diagram before the sections that follow.

Identity sits above the key registry, not beside it. A key is not the account; it is an entry in a registry bound to an identifier that exists independently of it. That single relationship is what makes §2.4 and §2.8 possible, and it is what a chain deriving addresses from public keys cannot express.

Everything below the identity layer is the identity-native ledger: one state, under one consensus. Identity is protocol state here, held on the same ledger as value rather than in a system beside it. Balances, identifiers, key bindings and governance are therefore not separate systems that must be reconciled. The alternative — accounts on-chain, the registry saying which key controls which account in a database or an oracle beside it — creates two systems that must agree but can disagree, and every interval of disagreement is where value leaves. Keeping them on one ledger is what makes the migration in §2.4 atomic rather than eventually consistent.

Personal data appears nowhere in the stack. It stops at the identity layer, held by the Identity Verifier (§2.7).

2.2 DID as the account primitive

The decision most chains made, and its consequences. On most blockchains an address is derived from a public key — typically a hash of it. This was an elegant decision and its virtues are real: accounts cost nothing to create, no registry has to exist, no authority issues anything, and anyone can transact without permission.

It also welds three separate things into one value. The **identifier** that receives funds, the **credential** that authorizes spending them, and the **cryptographic assumption** keeping the second from being derived from the first are all the same object. Change the key and the identifier changes with it, because the identifier was only ever a function of the key. Four consequences follow, and they are the reason this paper exists:

- **Key rotation requires moving assets** — not as an implementation detail, as arithmetic. A new key is a new address.
- **Loss is permanent.** If the key is gone, the account is gone. Proving who you are cannot help, because the chain never knew who you were.
- **Compliance sits outside the protocol.** The ledger records that an address moved value. It cannot record who did, having no representation of a who.
- **Post-quantum migration inherits all three.** The industry's problem is not choosing an algorithm — NIST chose the algorithms. It is that changing keys means moving every asset on the chain, by hand, one holder at a time.

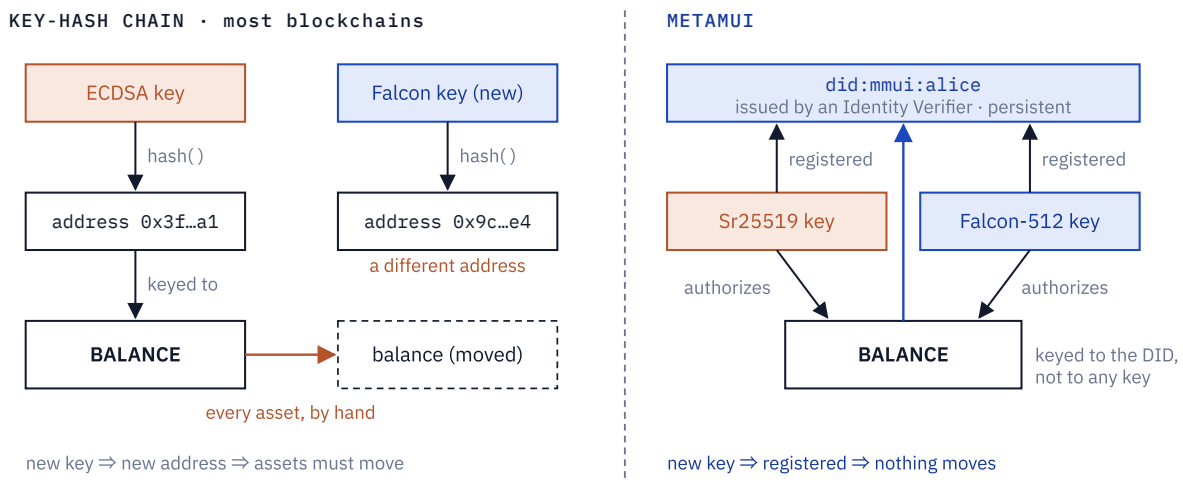

FIGURE 3 Two account models. On the left, identifier and credential are the same value, so changing the credential is moving the asset. On the right, the identifier is issued and persistent, keys are credentials registered against it, and the balance never references a key.

On MetaMUI the identifier is issued and persistent, and keys are credentials registered against it. Nothing about this makes the cryptography stronger. What it does is decouple the identifier from the key, and everything above changes as a result: rotation becomes a state change rather than a transfer (§2.4), loss becomes recoverable (§2.8), and post-quantum migration becomes a registration rather than a mass movement of value.

The difference is visible at the point of sale. A café in the deployment described in Part 4 prints its payment identifier on a card beside the till, and it reads `did:yidindji:mamadevi`. It is not an abbreviation of a longer string, and there is no longer string. That is the account.

> THE TRADE, STATED PLAINLY
>
> Accounts cannot be created permissionlessly. A DID is issued through a verifier, so the frictionless self-issued account creation key-hash chains offer does not exist here. That is a real cost, and it is deliberate. MetaMUI is built for regulated settlement, where the parties are already required to be known and an account no one is accountable for is an obstacle rather than a feature. For uses where permissionless account creation is the requirement, this is the wrong chain, and we would rather say so than pretend the design is free.

2.3 Multi-key identity

The chain operates as a decentralized public key infrastructure: it maintains the binding between an identifier and the public keys registered to it. Since the hard fork, **one identifier can hold several registered keys of different algorithms concurrently** — classical and post-

quantum together — and the verifier accepts any registered key valid for the operation.

This is the property that makes everything downstream possible. Migration (§2.4) is the registration of an additional key. Recovery (§2.8) is the registration of a replacement key. Neither is a special procedure; both are the same primitive invoked for different reasons.

It is also what required the hard fork, since accepting several algorithms is a change to what the verifier accepts (§2.0).

2.4 Classical-to-post-quantum key migration

Where everyone else stands. The landscape divides three ways, and the distinction is usually collapsed. Appendix B.2 gives the sourced detail.

Chains with no classical past. QRL has run mandatory XMSS signatures since 2018; Abelian, Tidecoin and Mochimo were likewise post-quantum from genesis, and in 2026 Naoris Protocol and Autheo launched mainnets post-quantum from their first block. These chains have no migration problem, because they never had a classical user base — a legitimate answer, available only to a chain starting from no users.

Chains migrating by hand. Bitcoin's holders must spend to a new output type themselves; a draft sunset proposal contemplates phasing out legacy signature types precisely because so many never will. Algorand's protocol-native Falcon-1024 accounts went live on mainnet in August 2026; they are opt-in and cleanly separated from classical accounts, so an existing holder creates a new account and funds it. Sui has announced a post-quantum scheme that would preserve existing addresses, targeted for 2027.

Chains designing an in-place path. Ethereum intends to upgrade accounts through account abstraction rather than transfers. The XRP Ledger already supports key rotation without an address change and targets 2028 for its post-quantum transition. Polkadot has proposed a post-quantum proof binding an existing account to a new key without moving value. Each is the right idea. None of the three is live.

Wherever it remains unfinished the consequence is the same: "safe" quietly becomes "safe, if everyone acts."

The migration invariant. Before describing the mechanism, the property it preserves, stated at the protocol level:

> *Asset state remains unchanged. Only credential state changes.*

A balance on MetaMUI is keyed to an identifier, not to a public key. Migration is a transition on the key-registry component of that identifier's state (§2.3). It reads no balance record, writes no balance record, transfers no value, and creates no account. The identifier is invariant across the operation, and because the balance is bound to the identifier rather than to any key, the balance is untouched by construction rather than by careful implementation.

On a chain where the address is derived from the public key, the identifier and the credential are the same object. Changing the credential therefore *is* moving the asset — not as a design choice that could have been made differently, but as an identity of terms. This is the whole of the difference.

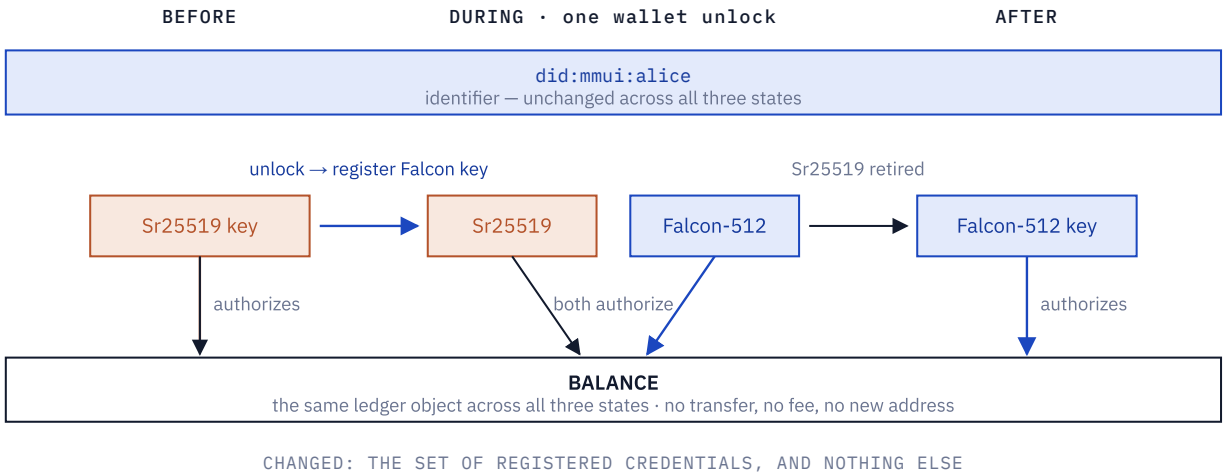

FIGURE 4 Migration as a key registration. The identifier and the balance are the same ledger objects before, during and after; only the set of registered credentials changes. Because the key binding and the balance are ordered by the same consensus, there is no interval in which the two disagree.

The mechanism: nothing the holder would not already be doing

1. The holder updates the app and unlocks the wallet the way they always do — biometric or PIN. That unlock produces the authorization, signed with the Sr25519 key they already hold. There is no separate migration screen, no additional confirmation, and nothing for the holder to understand.

2. The wallet generates a Falcon-512 key pair locally and registers the public key against the same identifier.

3. The identifier is unchanged. From that point the account authorizes transactions with a post-quantum signature.

The rotation is cryptographically authorized by the holder, as it must be. What is absent is any migration-specific action: the authorization is a by-product of ordinary use rather than a task the holder is asked to perform. Because the key binding and the balance are state on the same

ledger (§2.1), the rebinding is ordered by the same consensus that orders transfers — there is no interval in which a spend under the old key and a rebinding to a new one are both valid.

What does not happen at any step: no balance is transferred, no transaction carries funds anywhere, no new address is issued or memorized, no fee is paid to move value, and there is no interval during which a holder can be persuaded to send assets to a fraudulent "migration" address. The phishing surface every manual migration creates does not exist here, because there is nowhere for a user to send anything.

Holdings in custody. Exchanges, custodians, and other third parties hold balances under the same identifier model and register post-quantum keys the same way, on behalf of the balances they hold. A holder whose assets sit on an exchange does nothing at all.

What this does not claim. A holder who never opens their wallet again keeps their existing classical key, and that account remains classically secured. No protocol can rotate a key without an authorization from the party the key belongs to, so a permanently dormant account is a limit rather than a defect. What has changed is its size: the threshold is opening a wallet, not identifying a new address and transferring a balance to it. Part 5 states where this stands.

ASPECT	CHAINS MIGRATING BY HAND	METAMUI
Holder action	Send entire balance to a new address	**None beyond unlocking the wallet**
Address	Changes	Unchanged
Assets moved	All of them	None
Network fees	Paid per transfer	None
Phishing surface	A migration destination exists	None exists
Custodial balances	Holder must act	Custodian registers the key
If the wallet is never opened again	Funds remain exposed	Account remains classical
If the key is lost	Account lost permanently	New key bound to the same identity

2.5 Falcon-512 transaction signatures

Post-quantum signatures are larger than the elliptic-curve signatures they replace, and on a blockchain the cost compounds rather than adding. Part 1.2 gives the measured scale — a thirty-seven-fold increase in signature size and a 40% throughput loss in BNB Chain's published evaluation of ML-DSA-44. That is a defensible result for a general-purpose chain. It is not a defensible result for a settlement layer, where throughput and finality are the product.

Why Falcon-512. MetaMUI signs with Falcon-512, selected on signature size and verification cost rather than signing speed. Payment infrastructure verifies far more often than it signs: every node validates every signature in every block, while a given user signs occasionally.

Compact signatures with cheap verification are therefore the property that matters, and they are the property Falcon optimizes for — a Falcon-512 signature is roughly a quarter the size of an ML-DSA-44 signature.

The trade-off. Falcon is harder to implement correctly than ML-DSA, the lattice scheme it competes with; its sampling requires care to keep signing constant-time and side-channel resistant, and that implementation burden falls on us rather than on the standard. We accepted that cost because the alternative was accepting the throughput result above.

Standardization status. Falcon is being standardized by NIST as FN-DSA under FIPS 206, which remains at draft stage; the final standard is expected around the turn of 2027. We state this rather than describe Falcon as a finished NIST standard. Our implementation tracks the draft and will be reconciled with the final publication.

Measured performance. Measured from transaction submission to irreversibility, median finality on the identity main chain since the hard fork is approximately 65 ms, with a 99th percentile of approximately 524 ms — on a three-validator set in a single region. Appendix A gives the configuration and the sampling method, and is explicit that the throughput figure quoted there is derived from block occupancy rather than measured under sustained load. What these figures support is that post-quantum signing is not the bottleneck; they do not describe behaviour under load or under geographic distribution.

2.6 Post-quantum consensus

Security is determined by what the verifier accepts. This is the whole of the argument for why post-quantum cryptography must be protocol-native, and everything else in this section follows from it.

A wallet can generate any key it likes. It can generate a Falcon key, sign with it, and display a reassuring badge. If the network's verification rule still accepts a classical signature over that account, an attacker who can break the classical scheme does not need to defeat the post-quantum key — they present a classical signature and the network accepts it, because the rule says to. The post-quantum key protected nothing. It was decoration on an unchanged security boundary. The same reasoning applies to optionality: a chain is not quantum-safe when quantum-safety is available on it, but when it is not possible to transact on it any other way.

Signatures are not the stack. A chain whose users sign with post-quantum keys and whose validators agree on blocks using classical ones is protected exactly as well as its consensus layer — which is to say, not. An adversary who can forge the signatures validators exchange can finalize a block containing anything, and no property of user-level signing prevents it.

How MetaMUI reaches finality. MetaMUI runs a permissioned-public validator set: the network is public in that anyone may read it and transact on it, and permissioned in that block validation is performed by a registered set of known validators. That set — and its exact size —

is fixed and known at the start of each epoch. Blocks are produced on demand: a block is created when there are transactions to include rather than on a fixed interval. Finality is deterministic and single-block: once a majority of those registered validators have signed their finality votes, the block is irreversible, with no probabilistic confirmation period. Each validator signs its vote with a post-quantum key, so the agreement layer carries the same protection as the transaction layer.

The validator set is small. At the time of the measurements in Appendix A it comprised three validators in a single region. Because finality requires a majority of the registered set, blocks are finalized as long as two of the three are signing: the set tolerates one validator going offline, and no block is finalized by fewer than a majority. That is tolerance of an unavailable validator, not a Byzantine-fault-tolerance property, and an institution evaluating this chain should read it as such: the security of consensus rests on who the registered validators are rather than on their number. Part 5.3 records validator-set growth as an open item.

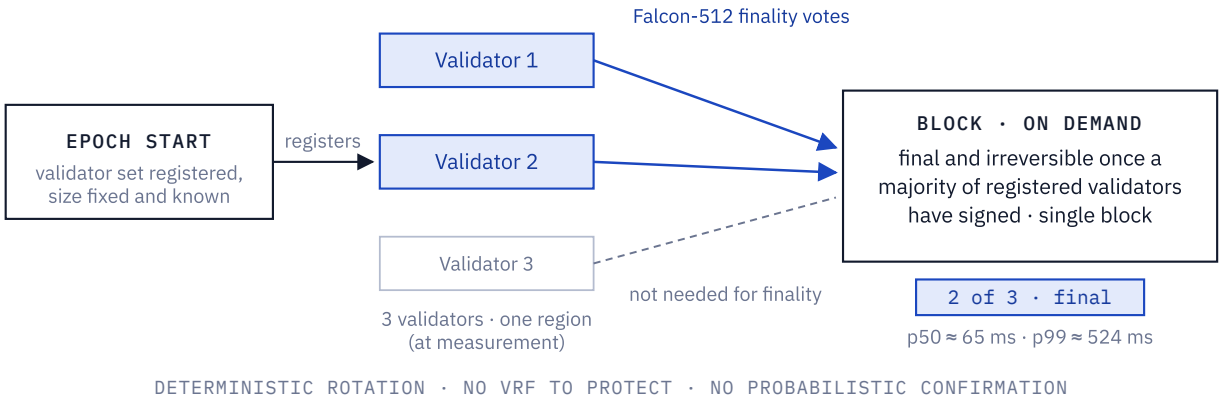

FIGURE 5 Finality on MetaMUI, drawn with the three-validator set on which the Appendix A measurements were taken. Each finality vote is a Falcon-512 signature; a block is final and irreversible once a majority of registered validators have signed. Proposer selection is deterministic because the validator set is fixed and known per epoch; there is no randomized election to protect.

Why there is no VRF here. A verifiable random function exists to make leader selection unpredictable. That requirement arises from a specific premise: a validator set that is open and changing, where any participant may join or leave, and where a publicly known next proposer would be a target to attack and a selection process would be something to game. MetaMUI does not operate under that premise. With the validator set fixed and its size known for the epoch, there is nothing for unpredictability to defend against — deterministic rotation suffices, and a majority of registered signatures is definitive rather than probabilistic.

This is not the hard problem solved. It is the hard problem not encountered, and the distinction matters. Chains with open validator sets need a quantum-safe VRF and do not yet have one; Algorand states plainly that its proposer-selection randomness and participation keys remain classical, with a post-quantum VRF still at the research stage, and Solana

describes replacing aggregated consensus signatures as an open problem. Those chains are solving for a property MetaMUI's design does not require — and they are carrying the permissionless validator participation that comes with it, which MetaMUI does not. Institutions evaluating this chain should evaluate that trade rather than the cryptography alone.

Two boundary cases complete the picture. Proof-of-work consensus uses no signatures, so a post-quantum proof-of-work chain has nothing to protect here — several clear this bar today, and they clear it honestly. And BNB Chain's evaluation is the only published attempt at an answer for open validator sets we found, aggregating validator votes through a post-quantum STARK. Appendix B.1 sets out each position with its source.

Measured performance. Finality percentiles and the measurement configuration are in Appendix A. Finality under load, and with a larger and geographically distributed validator set, has not yet been measured; it will be published from the demo network (Part 5.3).

2.7 The identity-native ledger

Three consequences of §2.1 matter concretely, and the third is the one institutions ask about first.

Rebinding is atomic with respect to balances. Covered in §2.4: because the key binding and the balance are ordered by the same consensus, there is no reconciliation window between them. On an architecture where identity is external, that window is a design problem to be mitigated. Here it does not exist to be mitigated.

Governance acts on the same state it governs. Validator registration, cross-chain approval, and issuance authority are ledger state under the same signatures and the same finality as everything else. The keyless protocol account in §2.9 is possible because there is one place where governance decisions and the assets they authorize both live.

Compliance is applied at the gate, and the ledger holds none of the evidence. MetaMUI is self-sovereign by design. Every DID is associated with an **Identity Verifier**: the party that performed the verification and that carries the compliance responsibility for it. The verification itself, and the personal data supporting it, remain with that verifier. The chain's role is to record the resulting identifier and its key bindings — to tokenize the outcome, not to store the evidence.

The consequence is that anti-money-laundering and sanctions obligations are discharged before an account exists, rather than re-evaluated on every transfer. An account on this ledger is an account that passed a verifier's process.

Two things follow, and both are worth stating plainly:

- **No personal data is written to an immutable ledger.** For institutions operating under GDPR-style erasure obligations this is not a convenience. A design that puts personal data on-chain and a right to erasure cannot both be satisfied; this one does not create the conflict.
- **The rigour of verification belongs to the verifier, not to us.** MetaMUI does not set, audit, or guarantee an Identity Verifier's standards, and verifiers will differ. A relying institution assesses a verifier here the same way it assesses any KYC reliance arrangement — by knowing who performed the verification and what they are answerable for. The architecture makes that attributable. It does not make it uniform, and we do not claim it does.

The ledger is therefore pseudonymous in its contents and attributable through its process, which are different properties and are usually confused. An observer reading the chain learns no more about a holder than on any other chain. An institution with a legal basis to ask can establish who an account belongs to, by going to the party that verified it.

2.8 Key recovery and rebinding

Because a key is a credential registered against an identity rather than the identity itself, the question "what happens if the holder loses their key?" has an answer here that key-hash chains cannot offer.

A Verifiable Credential issued by the Identity Verifier that established the account authorizes a new key to be bound to the same identifier. The account continues — same identifier, same balance, same history — under a new key. On a chain where the address is a hash of the public key, a lost key is a lost account, permanently, and no amount of proving who you are can change that, because the chain has no idea who you are.

Recovery is therefore not a feature layered onto migration. It is the same operation as §2.4 — rebinding an identifier to a different key — invoked for a different reason. Part 3.3 describes how a partner operating its own verification process issues these credentials.

This also answers the most reasonable objection an architect could raise against §2.4: if automatic migration and recoverable accounts are so clearly better, why has no one else shipped them? Because they are not features. They are consequences of identity being protocol state on the same ledger as value — and a chain that did not begin that way cannot adopt the consequences without becoming a different chain, which is what a hard fork is (§2.0).

2.9 Cross-chain dual-signature security

A chain can be quantum-safe at rest and still lose assets in transit. Bridges are where that happens, and they are the most exploited category in the industry: Chainalysis attributed roughly 69% of all cryptocurrency stolen in 2022 to bridge attacks. The largest individual

losses came from stolen signing keys rather than defective contract code — the Ronin bridge lost approximately $625 million when five of nine validator keys were compromised.

Two structural weaknesses recur:

1. **A small set of master keys authorizes every transfer.** Compromise enough and the bridge approves whatever the attacker wants, using entirely valid signatures.
2. **A single cryptographic system secures the transfer.** When it breaks — by key theft today, by cryptanalysis later — nothing is behind it.

NIST SP 800-53 control AC-5 requires that no individual hold sole control over a critical operation, so abuse requires collusion rather than a single compromised party. Most bridges are built the opposite way, and this is not an implementation defect but the design.

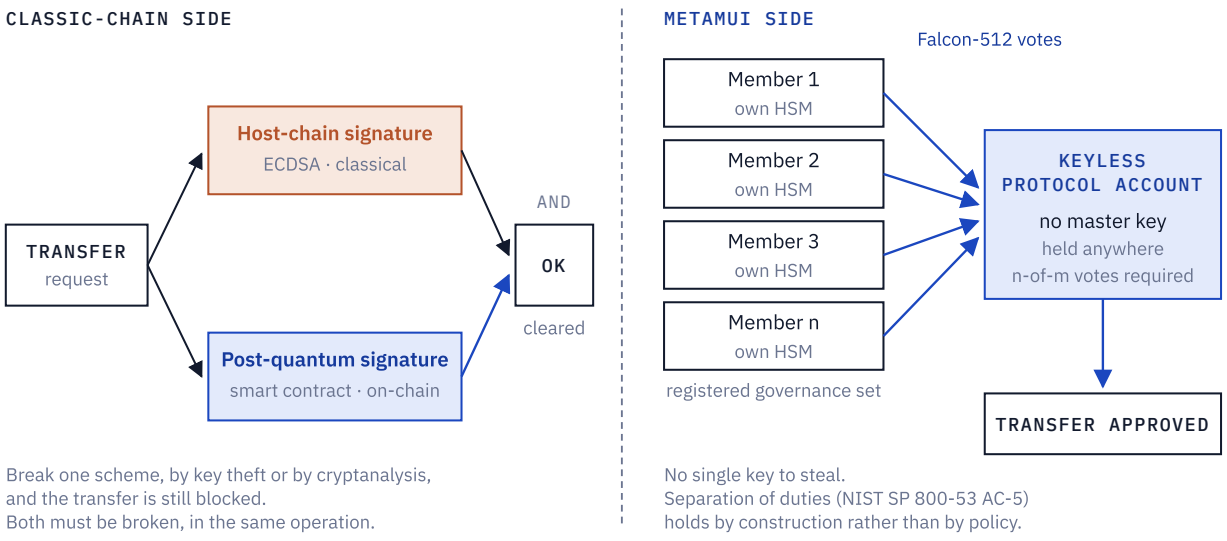

FIGURE 6 Cross-chain transfer authorization. On the classic-chain side, two independent cryptographic systems must both validate the same transfer. On the MetaMUI side, approval is a threshold of per-member hardware-module votes into an account that has no master key.

On the classic-chain side: two cryptographic systems, simultaneously. A transfer must clear the host chain's own signature scheme and a post-quantum signature enforced on-chain through a smart contract. Both must validate. An attacker cannot succeed by breaking elliptic-curve cryptography, and cannot succeed by breaking the post-quantum scheme; they must break both, in the same operation, against the same transfer. This also means assets on chains that will not complete their own migration for years can be protected while moving, without those chains changing anything.

On the MetaMUI side: no key to steal. Approval runs through a keyless protocol account. There is no master private key held anywhere. Each governance member votes with a post-quantum signature produced inside a hardware security module, and the transfer proceeds

only when the required votes are present. The single point of compromise that opened every recent bridge does not exist, and the arrangement satisfies AC-5 by construction rather than by policy.

What this still assumes. The design removes the master key, not the need for governance to be honest and available. Its security rests on the integrity of the registered governance set and the operational security of the hardware modules those members control. That is a materially stronger assumption than trusting a multisig wallet, and it is not the absence of an assumption. The composition of the governance set and the list of connected chains are not yet published; Part 5.3 records that. We are also not aware of any chain, ourselves included, operating an independently audited post-quantum bridge — Appendix B.3 says so plainly.

Part 3 Integration

MetaMUI is infrastructure, not a destination. This part documents what integration involves, what it does not involve, and where a prospective partner can test each claim before committing anything.

3.1 A completed system, not a construction kit

Most blockchains provide a virtual machine. An institution that wants to issue a token, settle a payment, or manage an account writes programs, deploys them, and lives with them. That model has produced a great deal of experimentation, and a category of loss that does not exist without it: defective contract code, and an audit obligation that never ends for as long as the code is deployed.

MetaMUI works the other way. It is delivered as an operated platform, closer in shape to a cloud service than to a programmable chain. Token issuance, identity, wallets, and settlement are existing functions of the running system, invoked through administration tools and SDKs rather than implemented as programs a partner writes and deploys. A partner issues a token in real time through the provided tools; there is no contract to compile, no contract to audit, and no deployment through which a defect can be introduced.

The consequence for a regulated institution is a smaller risk surface, and a differently shaped one. The question is no longer "is our contract correct?" but "is our integration correct?" — a question institutions already know how to answer, using controls they already operate.

> THE TRADE-OFF
>
> This is less sovereign than a permissionless virtual machine. Partners cannot deploy arbitrary on-chain logic, and functionality the platform does not provide cannot be added by the partner alone. For general-purpose experimentation that is a real cost. For regulated settlement, where the requirement is that the system behave identically every time and that its behavior be attestable to a supervisor, we consider it the correct trade. It remains a trade, and partners should evaluate it as one.

3.2 Integration models

Four ways in, in order of integration effort.

1. **Settlement lane.** Stablecoin issuers and payment providers add MetaMUI as one more supported chain — a decision they already know how to make — with the difference that value moving across it is quantum-safe by default rather than by user opt-in. Existing issuance, treasury, and reconciliation processes are unchanged.

2. **Withdrawal network.** An exchange adds MetaMUI as a withdrawal destination, allowing customers to withdraw into quantum-safe personal wallets. This requires no change to the exchange's internal custody model.

3. **Cross-chain protection.** Assets on chains that will not complete their own migration for years are protected while moving, through the dual-signature verification in §2.9. The originating chain changes nothing.

4. **Sovereign and institutional deployment.** A dedicated instance for a central bank, government, or regulated institution, with identity, issuance, and governance operated under that institution's control. Such a deployment is a separate, permissioned network running its own nodes rather than a shard of a shared chain, and its ledger is readable by its own account holders rather than by the public. For an issuer with data-sovereignty obligations that is the requirement, not a limitation.

3.3 What integration actually requires

What a partner builds

- **A wallet, if they want their own.** Partners operating a branded wallet build it with the MetaMUI Wallet SDK. Partners who do not can use the existing wallet.
- **An identity verification capability.** Because accounts are identities rather than key hashes, a partner issuing accounts acts as an Identity Verifier: it performs the verification, holds the resulting personal data, and carries the compliance responsibility for it. This is the same KYC obligation the partner already carries. What changes is that no part of it is written to the chain (§2.7).
- **Nothing else on-chain.** Token issuance runs through the administration tools MetaMUI provides, in real time. Consensus, DID structure, key management, and settlement are platform functions.

How identity connects to keys. The partner, as Identity Verifier, issues Verifiable Credentials. A VC is what authorizes a change to the binding between an identity and its registered public keys — the mechanism behind both migration (§2.4) and recovery (§2.8). The practical point for a partner is that the credential its own verification process issues is what lets a customer's account survive a lost device, and that this is the same operation the chain already uses to register a post-quantum key.

What a partner does not have to change. No smart contracts to write or audit. No custom consensus to operate. No replacement of existing custody, HSM, or treasury systems. No address format for customers to relearn. No dependency on customers performing a migration-specific action for the network's cryptographic guarantees to hold — migration completes on ordinary wallet use (§2.4; dormant accounts, Part 5).

3.4 Source availability, and where to test it

Verification of this paper's claims does not depend on a relationship with us, and it runs at three levels.

Public: the explorer. Whether the network is live, and whether it is finalizing blocks with post-quantum signatures, can be checked by anyone at any time.

Public: the source. The post-quantum cryptographic implementations, the Wallet SDK, and the blockchain core — including consensus and the DID structure — are published under the Business Source License. This is a source-available licence rather than an OSI-approved open source licence: the code may be read, audited, and evaluated, subject to the usage terms and the conversion schedule stated in the licence itself. The Change Date, Change Licence and Additional Use Grant are stated in the licence file in the repository rather than paraphrased here. For a reviewer, the practical point is that the cryptography this paper describes can be read rather than believed.

On request: the demo network. The demo network opens in September 2026. Hands-on access will be provided to institutions and other chains by request or invitation. What can be exercised there:

- Finality under load, and post-quantum signature verification cost
- DID issuance, and registration of a post-quantum key against an existing identity
- Wallet reset and public key rebinding through a Verifiable Credential
- Real-time token issuance through the administration tools
- Cross-chain dual-signature approval

Offline payment is not yet part of this list; Part 5 states where it stands.

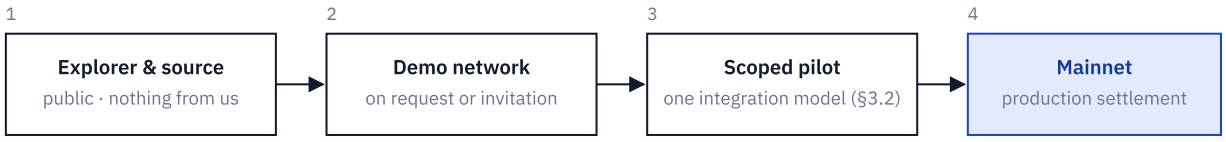

FIGURE 7 The path in. The first stage requires nothing from MetaMUI at all, which is deliberate: a claim that can only be checked by asking its author is not much of a claim.

The path in. Explorer and source review, then demo network, then a scoped pilot, then mainnet. The first stage requires nothing from us at all — which is deliberate, because a claim that can only be checked by asking its author is not much of a claim.

→ explorer.metamui.id → github.com/SovereignWallet-Network

Demo network — opening September 2026 → Appendix A

Part 4 Deployment Status

MetaMUI is built by SovereignWallet, headquartered in Seoul; its Singapore entity appears in some of the sources below as SWN Global.

4.1 What has actually run

A government currency, in commercial use since 2022. A digital currency issued by the Sovereign Yidindji Government, a self-governing Aboriginal nation in Queensland, Australia, has run on MetaMUI since January 2022 and is accepted by around thirty merchants in the Yidindji commercial area. It runs as a separate instance on the previous architecture and is not quantum-safe; we include it because four years of ordinary retail payments is evidence about the identity architecture rather than about the cryptography. The launch was reported independently at the time by Forkast and by Australia's public broadcaster SBS NITV (Appendix D).

Central bank infrastructure work. This paper's first author, together with MetaMUI's chief strategy officer for CBDC, is named in the Bank for International Settlements Innovation Hub's May 2023 handbook on offline payments with CBDC, among the private-sector practitioners interviewed for it — alongside Visa, Ripple, Thales, Giesecke+Devrient, IDEMIA and NTT Data. In the Innovation Hub's deep-dive sessions that year, SovereignWallet presented its offline payment design to Hub staff and observing central bank representatives, and demonstrated a completed payment between two devices with both placed in airplane mode. The design was published in the Hub's October 2023 guide, in which SWN Global is listed among the solution vendor participants.

A central bank pilot shortlist. In 2023 SovereignWallet was one of nine technology providers shortlisted by the National Bank of Georgia for its Digital GEL pilot.

What we are not listing. Discussions with financial institutions are ongoing. We do not name them, because a discussion is not a deployment, and a paper that treats the two as equivalent is not worth reading. When something is running, it will appear here.

4.2 What the architecture is suited for

The following are properties of the design rather than a customer list. Each is stated with the reason quantum-safety is relevant to it, because a use case that works equally well without it does not belong in this paper.

Regulated payments and settlement. Stablecoin settlement, cross-border transfer, and securities settlement share a requirement general-purpose chains treat as optional: every party must be attributable, and settlement must be final in seconds. Value in these systems has a long life — a settled security or a cross-border position may sit for years — which makes harvest-now-decrypt-later a present concern rather than a future one, and makes migration that depends on holders acting individually unworkable at institutional scale.

Central bank and sovereign issuance. Issuance authority, identity, and governance operate as protocol state under an institution's own control, and no personal data reaches the ledger — a constraint most public-chain designs cannot satisfy under GDPR-style erasure obligations (§2.7). A currency is also the clearest case where migration cannot be delegated to users: a central bank cannot instruct a population to move their holdings by hand.

Enterprise treasury and regulated instruments. Corporate holdings are long-lived, custody is delegated, and key loss is an operational event rather than a personal tragedy. Identity-bound keys mean a lost or compromised key is rebound rather than written off, and custodians migrate on behalf of the balances they hold without customer action (§2.4).

Part 5 Roadmap, Verification, and Known Limitations

5.1 Where things stand

HARD FORK ACTIVATED	POST-QUANTUM SIGNING	UPDATED WALLET
Block 35,499,408 13 September 2026, 08:00 KST	Transaction · Consensus Falcon-512 on both paths	Android · iOS Holders migrate on unlock

The hard fork activated at block 35,499,408 on 13 September 2026, 08:00 KST. The network is in production with post-quantum signing active at both the transaction and consensus layers, and mainnet identifiers have migrated automatically from `did:ssid:` to `did:mmui:`.

The updated MetaMUI wallet is available on both Android and iOS. Holders are migrating as they update: a Falcon-512 key is registered against the existing identifier when the wallet is unlocked, and no balance moves. The mechanism described in §2.4 is not a design intention in this paper — it is what the network has been doing since activation, and it is visible on the explorer.

5.2 How to check any of it

- **The explorer** — that the network is live and finalizing with post-quantum signatures. Public: explorer.metamui.id
- **The source** — the post-quantum implementations, the Wallet SDK, and the blockchain core including consensus and the DID structure, published under the Business Source License for review. Public: github.com/SovereignWallet-Network
- **The demo network** — hands-on testing of finality under load, DID issuance and key registration, key rebinding by Verifiable Credential, real-time token issuance, and cross-chain dual-signature approval. Opening September 2026, available to institutions and other chains on request via the contact published with this paper.

5.3 What is not finished

A paper that lists only what works is an advertisement. These are the open items as of publication.

Dormant accounts `IRREDUCIBLE LIMIT`	Migration completes when a holder unlocks their wallet, which requires no migration-specific action but does require the wallet to be opened. An account that is never opened again keeps its classical key. No protocol can rotate a key without an authorization from its holder, so this is a limit rather than a defect — the residue of the problem Part 1 describes, reduced to its irreducible core. There is no grace period, because there is no separate step to grant time for.
Offline payment `NOT ON MAINNET`	Demonstrated on the previous architecture in 2023 and being restored on the rebuilt chain — demo network first, then mainnet. Quantum-safe operation was sequenced ahead of it. As of this paper, offline payment is not available on mainnet.
Falcon standardization `FIPS 206 DRAFT`	Falcon is being standardized as FN-DSA under NIST FIPS 206, which remains at draft stage. Our implementation tracks the draft and will be reconciled with the final publication. Until then, this paper does not describe our signature scheme as a finished NIST standard.
Verifier standards vary `BY DESIGN`	Identity verification is performed by Identity Verifiers, who carry the compliance responsibility for it. MetaMUI does not set or audit their standards, and their rigour will differ (§2.7).
Randomized proposer selection `NOT ENCOUNTERED`	Chains that select block proposers by verifiable random function need a quantum-safe VRF, which remains unsolved. MetaMUI's permissioned-public validator set means the architecture does not encounter this problem. It does not mean the problem is solved (§2.6).
Validator set size and distribution `NOT MEASURED`	The measurements in Appendix A were taken on three validators in a single region. Finality under a larger, geographically distributed set has not been measured, and validator-set expansion is not yet on a published schedule.
Governance set and connected chains `NOT PUBLISHED`	The composition, quorum and selection method of the cross-chain governance set are not yet published, nor is the list of connected chains. Both belong in Appendix A and will appear there.

Signature verification time and throughput under load NOT MEASURED	Post-quantum signature verification cost has not yet been measured and published; neither has sustained throughput. Median and tail finality are measured (Appendix A). Sustained throughput is not: the figure in Appendix A is derived from block occupancy and median finality. Load testing will be run on the demo network and the result published here, whatever it shows.
Independent audit of the cross-chain design NOT AUDITED	We are not aware of any chain operating an independently audited post-quantum bridge, and that includes ours (Appendix B.3).
The previous architecture is still running PRE-FORK RUNTIME	The Yidindji deployment described in Part 4.1 remains on the pre-fork runtime and is not quantum-safe. Bringing it to the current architecture would require its cryptographic layer to be built out separately. No date has been set for that work.

5.4 Next

Publication of the core under the Business Source License, then partner pilots on the demo network, then offline payment on mainnet. No dates are published for the last two; they will appear here when they are fixed.

We document what is running. Where something is in progress, this paper says so — the section above is that commitment, kept.

Appendix A Technical Specification

FINALITY · P50	FINALITY · P99	THROUGHPUT	CONFIGURATION
≈ 65 ms	≈ 524 ms	≈ 2,950 TPS	3 validators
Submission to irreversibility	Deterministic, single block	Derived, not load-tested	Single region

CRYPTOGRAPHY	
Signature scheme (user)	Falcon-512
Signature scheme (consensus)	Falcon-512, validator finality votes
Signature size	Falcon-512 — approximately 666 bytes (variable length)
Standardization status	FN-DSA, NIST FIPS 206 — draft; final expected around the turn of 2027
Legacy scheme retained	Sr25519, for accounts not yet rebound
Multi-algorithm verification	Yes — one identifier may hold several registered keys concurrently
IDENTITY AND STATE	
Account model	DID; account is the identifier, keys are registered credentials
Identifier namespace	`did:mmui:`
Identity data on-chain	None. Verification held by the Identity Verifier (§2.7)
On-chain state (identity-native ledger)	Identifiers, key bindings, balances, governance — one state under one consensus
CONSENSUS AND PERFORMANCE	
Consensus	Permissioned-public; validator set registered per epoch; deterministic single-block finality by a majority of the registered set (2 of 3 at measurement); no block is finalized by fewer than a majority
Proposer selection	Deterministic rotation over a set fixed and known per epoch; no verifiable random function (§2.6)
Block production	Event-driven: a block is produced when there are transactions to include. No fixed block interval; see note below
Hard fork activation	Block 35,499,408 · 13 September 2026, 08:00 KST
Finality	Deterministic, single block. p50 ≈ 65 ms · p99 ≈ 524 ms — see measurement note
Throughput	≈ 2,950 TPS **derived** — see note below

Signature verification time	Not yet published — see Part 5.3
Validator set at measurement	3 validators, single region
CROSS-CHAIN	
Cross-chain (classic side)	Dual signature: host-chain scheme + on-chain post-quantum signature
Cross-chain (MetaMUI side)	Keyless protocol account; per-member HSM post-quantum votes
Governance set	Composition, quorum and selection are not yet published — see Part 5.3
Connected chains	Cross-chain connections are being brought up; each will be listed here as it is enabled
VERIFICATION	
Explorer	explorer.metamui.id
Source repository	github.com/SovereignWallet-Network
Source availability	Business Source License — PQC implementations, Wallet SDK, core
BSL parameters	As stated in the licence file in the repository

On the throughput figure. The 2,950 TPS above is derived, not measured under load: an observed block of 192 transactions reaching finality in the 65 ms median implies approximately 2,950 transactions per second. We publish the derivation rather than the number alone because the two are not the same claim — and because on an event-driven chain, block occupancy is not a steady-state property.

Why there is no block interval to report. MetaMUI is event-driven: it produces a block only when there are transactions to include. The time between blocks therefore reflects when transactions arrive, not a property of the chain, and it does not mean what block time means on a chain that produces blocks on a fixed schedule. A quiet period produces no blocks at all, and a burst of transactions produces blocks as fast as they finalize. The time that describes the network is the one a transaction experiences — submission to irreversibility — and that is the 65 ms median reported above. Sustained throughput under load will be measured on the demo network and published here when it is.

What the finality figures measure, and in what configuration. The interval is from transaction submission to irreversibility. MetaMUI provides deterministic finality: a block is final once a majority of registered validators have signed their finality votes, in a single block, with no probabilistic confirmation period to wait out.

The configuration matters and we state it rather than leave it to be inferred. The measurement was taken on a **three-validator set in a single region**, on a chain that produces blocks only when there are transactions to include, with the sample drawn over a short window at block-

production times rather than continuously. A small, co-located validator set is a large part of why the figure is what it is.

What the number therefore supports is narrower than "the network is fast," and is the claim we are actually making: **post-quantum signing is not the bottleneck.** Falcon-512 signature generation and verification, at both the transaction and consensus layers, leave deterministic finality inside 100 milliseconds at the median in this configuration. What it does not establish is behaviour under load, under geographic distribution, or with a larger validator set. Those are in Part 5.3 as open items.

Comparative benchmark. The reference figures cited in Part 1.2 and §2.5 are BNB Chain's published evaluation of ML-DSA-44 (Appendix D, ref. 4): signature 65 → 2,420 bytes; native transfer ~110 bytes → ~2.5 KB; block ~130 KB → ~2 MB; cross-region native-transfer throughput 4,973 → 2,997 TPS; gas throughput halved. That evaluation is an engineering assessment, not a mainnet or public-testnet deployment, and we describe it as such.

Appendix B Where Chains Stand

Every cell is sourced in Appendix D. Status is as of 15 September 2026 and will age; the sources are dated so a reader can check what has moved. Where we could not verify a claim, the cell says so rather than guessing — including for chains whose own materials assert more than we could confirm independently.

B.1 Post-quantum status

CHAIN	PQ LIVE ON MAINNET	SCHEME	CONSENSUS LAYER	STATED TARGET
MetaMUI	Yes — since 13 Sep 2026	Falcon-512	Falcon-signed finality votes	—
Bitcoin	No	BIP-360 (P2MR) merged as a document	n/a — proof-of-work	None stated
Ethereum	No	Research; devnets	Planned: BLS → hash-based, STARK-aggregated	~2029 core PQ
Solana	No — third-party opt-in vault only	Falcon under evaluation	Described as unsolved	None stated
BNB Chain	No — engineering evaluation	ML-DSA-44	pqSTARK vote aggregation	None stated
XRP Ledger	No	ML-DSA under test	Thin detail	2028
Cardano	No	Research programme	Proposed: PQ VRF, KES	Research only, to end-2026
Tron	No — public testnet	Falcon-512 / ML-DSA-44	Not addressed	Not fixed
Polkadot	No — proposal	ML-DSA / Falcon proposed	Proposed incl. PQ beacon	None stated
Avalanche	No public initiative found	—	—	—
Algorand	**Yes** — Falcon state proofs since 2022; native Falcon-1024 accounts since Aug 2026	Falcon-1024	**Classical** — VRF and participation keys; PQ-VRF paper targeted early 2027	End-2027
QRL	Yes — since 2018	XMSS	n/a — proof-of-work	—
Abelian · Tidecoin · Mochimo	Yes — from genesis	Lattice / Falcon-512 / WOTS+	n/a — proof-of-work	—

CHAIN	PQ LIVE ON MAINNET	SCHEME	CONSENSUS LAYER	STATED TARGET
Cellframe	Yes — claimed	Multi-scheme	Claimed; independently unverified	—
QoreChain	Claimed — since Jun 2026	ML-DSA-87	Claimed; independently unverified. EVM lane classical	—
Naoris Protocol	Claimed — since Apr 2026	NIST lattice suite (ML-DSA per own materials); EVM-compatible	dPoSec, invite-only validator set; claimed, independently unverified	—
Autheo	Claimed — since May 2026	ML-DSA / SLH-DSA, ML-KEM (per own materials); W3C DID identity	Claimed; independently unverified	—
Circle Arc	No — post-quantum support stated for mainnet launch, opt-in	Not named	Deferred to last	None stated
Sui	No — announced Aug 2026	ML-DSA-65 · SLH-DSA	Not addressed	2027
Tezos	No — previewnet announced Sep 2026	ML-DSA-44	Proposed: STARK-aggregated hash signatures	None stated
Quantus	Yes — mainnet 10 Sep 2026, greenfield	ML-DSA-65 / ML-DSA-87	n/a — proof-of-work	—

B.2 Migration of existing holders

CHAIN	HOLDER ACTION	ADDRESS	ASSETS MOVED	POLICY FOR THOSE WHO NEVER ACT
MetaMUI	**None beyond unlocking the wallet**	Unchanged	None	Dormant accounts stay classical (Part 5)
Bitcoin	Spend to a new output type	Changes	All	Draft sunset proposal, phased
Algorand	Create and fund a new opt-in account	Changes	All	Not found
Sui	Address preserved — announced, not live	Unchanged (planned)	None (planned)	Not found
Ethereum	Wallet-guided upgrade — not live	Unchanged (planned)	None (planned)	Not found
XRP Ledger	Key rotation — PQ not live	Unchanged	None	Not found

CHAIN	HOLDER ACTION	ADDRESS	ASSETS MOVED	POLICY FOR THOSE WHO NEVER ACT
Polkadot	PQ proof of shared seed — proposed	Unchanged (proposed)	None (proposed)	Not found
BNB Chain	Address format retained — not deployed	Unchanged (planned)	None (planned)	Not found
Tron	Create a new PQ wallet — testnet	Changes	All	Not found
Circle Arc · Quantus	New chains — opt-in / PQ from genesis	n/a	n/a	n/a — no legacy holders
QRL · Abelian · Tidecoin · Mochimo · Naoris · Autheo	None — PQ from genesis	n/a	n/a	n/a — no classical era

> Two observations we would rather state than leave implied. First, chains that were post-quantum from genesis have no migration problem at all; that is a real answer, available to a chain beginning with no users. Second, a published policy for holders who never migrate is absent almost everywhere — including, in its irreducible form, here (Part 5.3).

B.3 Cross-chain

We found no chain in this survey operating a documented, independently audited post-quantum bridge. Wrapped representations — QRL's ERC-20, wrapped CELL, wTDC, QANX — remain secured by the host chain's classical cryptography whatever the native chain's posture. MetaMUI's dual-signature design is described in §2.9; it has not been independently audited either, and we say so.

Appendix C Standards

STANDARD	STATUS HERE
NIST FIPS 206 / FN-DSA (Falcon)	Implemented per draft. **Not a final standard** — see Part 5.3
NIST FIPS 204 / ML-DSA	Not used. Rationale in §2.5
NIST SP 800-53 AC-5 — separation of duties	Cross-chain governance designed to it (§2.9)
NIST IR 8547 — PQC transition	ECDSA/RSA deprecated after 2030, disallowed after 2035 (initial public draft)
W3C Decentralized Identifiers	Conformance assessment not yet published
W3C Verifiable Credentials	Conformance assessment not yet published
ISO / other	None claimed

Appendix D References

Threat and transition timeline

1. Lang, Hannah. "Crypto firms prepare defenses as quantum threat to encryption draws nearer." *Reuters*, 8 July 2026.
2. "Bitcoin may take 7 years to upgrade to post-quantum: BIP-360 co-author." *Cointelegraph Magazine*, 18 February 2026.
3. NIST IR 8547 ipd, *Transition to Post-Quantum Cryptography Standards*, November 2024, Table 2.

Performance

4. *BSC Post-Quantum Cryptography Migration Report*, BNB Chain, 14 May 2026.

Bridge security

5. Chainalysis, *2022 Crypto Crime Report* — bridge attacks as a share of value stolen.
6. NIST SP 800-53 Rev. 5, control AC-5.

Chain status (Part 1.1 and Appendix B)

7. bip360.org; BIP-361, *Post Quantum Migration and Legacy Signature Sunset* (draft).
8. Milton & Shikhelman, *Bitcoin Post-Quantum*, Chaincode Labs, May 2025.
9. pq.ethereum.org; ethereum.org/roadmap/future-proofing; EIP-7932 (draft).
10. *Protocol priorities*, Ethereum Foundation, 7 September 2026.
11. *Solana's Quantum Readiness*, Solana Foundation, 27 April 2026.
12. *Post-Quantum Readiness on the XRP Ledger*, Ripple, 20 April 2026.
13. *Cardano Vision 2026*, IOG, 19 June 2026.
14. *Trying TRON Post-Quantum Signatures on the Testnet*, TRON Core Devs, 3 July 2026.
15. *Post-Quantum Cryptography Roadmap for Polkadot and JAM*, Web3 Foundation, 5 June 2025.
16. algorand.co/technology/post-quantum; *Algorand v5.0.0*, August 2026.
17. theqrl.org/roadmap.
18. *Arc's Quantum-Resistant Design and Roadmap*, 2 April 2026.
19. *Arc Mainnet Goes Live on September 16, 2026*, Arc, 5 August 2026.
20. Sui post-quantum signature scheme announcement, August 2026.
21. *Why post-quantum, why now*, Tezos, 2 September 2026.
22. Quantus mainnet launch, 10 September 2026.
23. "Naoris Protocol's quantum-resistant blockchain goes live as Bitcoin and Ethereum face 'Q-Day' threats." *CoinDesk*, 3 April 2026; Naoris Protocol mainnet announcement, 1 April 2026.

24. "Autheo launches quantum-proof mainnet as crypto braces for cryptographic threat." *TheStreet*, May 2026; Autheo mainnet live 14 May 2026.

Deployment record (Part 4)

25. *A handbook for offline payments with CBDC, Part 1: Project Polaris*, BIS Innovation Hub, May 2023, p. 88.
26. *A high-level design guide for offline payments with CBDC*, BIS Innovation Hub, October 2023, p. 38.
27. "The National Bank of Georgia plans to select a single Technology Partner for the Digital GEL pilot project," NBG, 28 September 2023.
28. Keller, Lachlan. "Territory in northeastern Australia launches own CBDC." *Forkast*, 31 January 2022. Names MetaMUI as the network.
29. Jenkins, Keira. "Sovereign Yidindji Nation launches digital currency." *SBS NITV*, 2 February 2022. Interview with the Yidindji Financial Technology Minister; does not name the network.
