Physical-Layer Cryptographic Authorization for Secure Cryptocurrency Infrastructure

A Hardware-Rooted Architecture for Securing Blockchain Control-Plane Operations

Document Type	White Paper
Author	Chris M. Hymel, Ph.D. Analog Guard®, Inc.
Date	March 2026
Subject	Hardware-rooted physical-layer cryptographic authorization for securing cryptocurrency control-plane operations
Primary Audience	Digital asset infrastructure operators, custody platforms, DeFi protocol teams, bridge developers, auditors, security architects, institutional stakeholders, and policy reviewers
Keywords	Cryptocurrency Security; Blockchain Control-Plane Security; Hardware Security; Physical-Layer Cryptography; Authorization Systems; Digital Asset Infrastructure

Core proposition:

Privileged blockchain authority can be grounded in verified real-time physical behavior rather than in a portable digital credential.

Executive Summary

Modern cryptocurrency infrastructure depends on cryptographic authorization mechanisms to approve high-impact control-plane operations such as token issuance, cross-chain asset releases, governance execution, validator management, and institutional custody transfers [3]. Blockchain consensus can preserve ledger integrity, yet many of the ecosystem's largest losses have originated elsewhere: in the systems and workflows that determine which privileged actions may be initiated at all [4], [5].

That distinction matters. A blockchain may function exactly as designed while still executing a malicious but cryptographically valid instruction if the authorization pathway behind that instruction has been compromised. Hardware security modules, multi-signature schemes, trusted execution environments, and custody workflows can reduce risk, but they still center authority on digital credentials that can be misused if surrounding infrastructure, operators, or workflows fail [10]-[13].

This paper proposes a different authorization model. Instead of treating authority as a stored digital secret, it derives authorization from the verified real-time physical behavior of a dedicated hardware device. The device generates continuously evolving signals through nonlinear analog or mixed-signal dynamics. An observation subsystem measures those signals, extracts features describing the device's current behavior, and verifies that the device remains in a verified physical state established during enrollment.

Authorization is produced only when three conditions are satisfied simultaneously: first, the device is in a verified physical state; second, the requested blockchain action satisfies protocol-level and policy-level constraints; and third, the canonical operation message is bound to the device's instantaneous physical state through a message-physics transformation. In this framework, authority exists only as a transient, device-bound condition rather than as a portable credential that can be exported, replayed, or reused outside the approved hardware environment.

The resulting authorization artifact accompanies a blockchain transaction and is verified before privileged control-plane operations are executed. This design allows the architecture to function as an overlay security layer for existing cryptocurrency systems rather than as a replacement for blockchain consensus. The same approach can be applied to stablecoin issuance systems, cross-chain bridges, governance execution frameworks, validator and oracle admission controls, and institutional custody platforms [6]-[10], [16], [17].

The broader significance of the architecture is that it shifts the root of trust for sensitive blockchain operations away from possession of a reusable digital secret and toward demonstration of verified real-time physical integrity under policy control. In that sense, it offers a hardware-rooted security primitive for cryptocurrency control-plane authorization that

is designed to raise the difficulty of key theft, replay, emulation, and surrounding-infrastructure compromise while remaining compatible with existing blockchain environments.

Key Takeaways

- The primary weakness addressed is cryptocurrency control-plane authorization, not blockchain consensus itself.
- Many privileged blockchain actions still depend on portable digital credentials, even when protected by advanced custody or key-management systems.
- The proposed architecture derives authorization from verified real-time physical hardware behavior rather than from persistent signing authority.
- Authorization occurs only when verified physical state, policy compliance, and message-physics binding are satisfied simultaneously.
- The architecture can be deployed alongside existing blockchain systems as a hardware-rooted control-plane security layer without changing consensus protocols.

White Paper Orientation

Problem	High-impact blockchain operations remain exposed when privileged authority is represented as a portable digital credential.
Proposed Architecture	A hardware-rooted authorization appliance verifies device behavior and policy conditions before producing an authorization artifact.
Security Shift	Authority is treated as a transient device-bound approval condition rather than a reusable secret.
Verification Path	A privileged action proceeds only when the operation message, the artifact, and the verified physical state correspond under the applicable policy conditions.
Deployment Areas	Stablecoins, bridges, governance systems, validator and oracle controls, and institutional custody workflows.

Contents

1. Introduction

Blockchain systems were introduced to reduce dependence on centralized trust by combining distributed consensus with cryptographic verification [1]-[3]. That model is powerful, but it secures only part of the operational stack. Many of the most consequential actions in cryptocurrency infrastructure arise not from ordinary end-user transaction flow, but from privileged operational processes that govern asset issuance, cross-chain release, governance execution, validator admission, and custody movement [4], [5].

Over time, blockchain networks have evolved far beyond simple peer-to-peer payment systems. Modern cryptocurrency ecosystems now support decentralized financial markets, tokenized assets, programmable smart contracts, cross-chain interoperability mechanisms, governance frameworks, oracle-dependent execution paths, and institutional custody platforms. Within these systems, many critical actions occur outside the ordinary flow of user transactions processed by the consensus layer. Actions such as token minting and burning, bridge releases, governance-driven upgrades, validator admission, and large custody withdrawals require explicit authorization before they can be executed on-chain.

These functions form the control plane of cryptocurrency infrastructure. Consensus determines how transactions are validated and incorporated into the ledger. The control plane determines which high-impact operations may be initiated in the first place. In practice, it governs the economic and operational boundaries of a blockchain system, including issuance of assets, movement of funds across networks, and modification of core protocol logic.

The same structural problem appears in different forms across several major parts of the digital asset ecosystem, including issuance systems, bridges, governance execution, and custody operations. Across much of that ecosystem, control-plane authority is still expressed through administrative private keys, validator credentials, distributed key shares, or similar digital constructs. Even when these credentials are well protected, they remain reusable sources of authority. If an attacker gains sufficient access to the systems, people, or workflows surrounding them, the blockchain will often accept the resulting instructions as valid because the network sees only a correct credentialed action, not the operational legitimacy behind it [5], [10].

This reliance on portable digital authority creates a persistent structural vulnerability. Credentials can be copied, extracted, coerced, replayed, or misused if the surrounding operational environment is compromised. Once an attacker obtains sufficient signing authority, the blockchain protocol generally cannot distinguish between legitimate and malicious instructions, because both appear as cryptographically valid transactions. The control-plane security problem is therefore not primarily that consensus fails. It is that privileged authorization can be separated from the real operational, physical, and policy conditions under which approval should occur.

This paper addresses that structural weakness by proposing a physical-layer cryptographic authorization architecture. The architecture does not attempt to replace blockchain consensus or conventional cryptography in general. Instead, it inserts a hardware-rooted

authorization layer at the point where privileged operations are approved. Under this model, authorization derives from verified real-time physical behavior of a dedicated device operating within defined policy constraints.

The central claim is straightforward: for the most sensitive blockchain actions, authority need not reside in possession of a portable digital secret. It can instead be tied to a live, measured, and continuously changing physical process that must be present and verified at the time approval is granted. In this model, authority is not merely stored and invoked. It is demonstrated under controlled conditions as a transient, device-bound approval event.

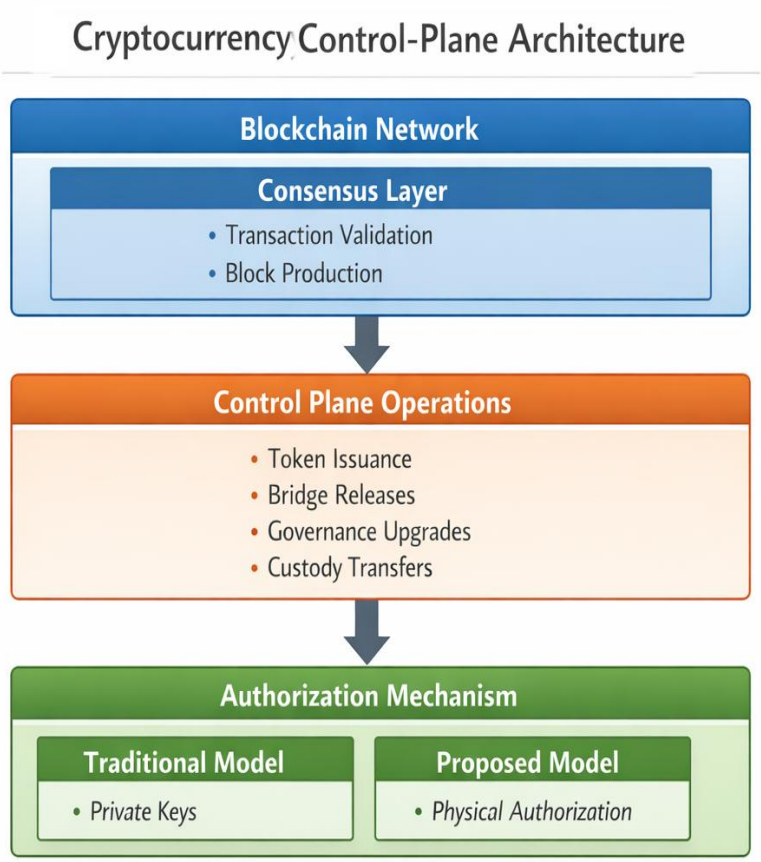
The proposed framework replaces static signing authority in the privileged authorization path with a hardware-rooted process derived from the real-time physical dynamics of a dedicated device. A nonlinear physical module generates continuously evolving signals whose properties are observed and evaluated through signal analysis and feature extraction. Authorization is produced only when the device is in a verified physical state, the requested blockchain action satisfies protocol-level and policy-level constraints, and the canonical operation message is bound to the device's instantaneous physical state through a message-physics transformation. The resulting authorization artifact accompanies the blockchain transaction and is verified before privileged actions are executed. Through this mechanism, authorization becomes materially harder to extract from its intended context than in conventional private-key-based control paths.

Beyond addressing specific vulnerabilities in cryptocurrency infrastructure, the architecture introduced in this work reflects a broader shift in how digital authorization may be established. Conventional cryptographic systems derive authority from possession of persistent digital credentials. In contrast, the framework proposed here derives privileged authorization from the verified real-time behavior of a physical system. This shifts authority from a static credential model toward a time-dependent physical approval model anchored in observable device behavior.

The primary contributions of this work are as follows.

1. It introduces a physical-layer cryptographic authorization architecture for securing the control plane of cryptocurrency systems, replacing portable private-key authority in the privileged authorization path with hardware-rooted verification of real-time physical behavior.
2. It defines a message-physics binding mechanism that couples canonical blockchain operation messages with features derived from the authorization device's instantaneous state, producing authorization artifacts that are specific to the approved message and approval event.
3. It presents a system model, adversary analysis, and implementation framework showing how the architecture can be integrated with existing blockchain infrastructures to secure critical operations such as token issuance, bridge releases, governance upgrades, validator and oracle controls, and institutional custody transfers.

The relationship among the consensus layer, privileged control-plane operations, and the transition from conventional credential-based approval toward physical-layer authorization is illustrated in Figure 1.



For clarity, several terms are used consistently throughout this paper. The authorization appliance refers to the complete hardware and software environment responsible for authorization decisions. The authorization device denotes the hardware element within that appliance that performs physical-state verification and artifact generation. Within the device, the physical module refers specifically to the signal-generating subsystem responsible for producing the time-varying behavior used for verification. The authorization artifact is the evidence object that accompanies a blockchain transaction and serves as verifiable proof that a privileged operation was approved under the required conditions.

The sections that follow define that control-plane weakness in practical terms, describe the proposed authorization architecture, formalize its operating condition, analyze its security posture, and examine implementation, policy, and future research implications.

2. System Overview

The proposed system introduces a hardware-rooted authorization layer positioned between privileged operational workflows and the blockchain transactions that implement those workflows. Rather than authorizing sensitive actions by invoking a stored signing key, the system determines whether a dedicated authorization device is in a verified physical state and whether the requested operation satisfies applicable protocol and policy constraints.

The architecture consists of four primary functional elements: a nonlinear physical module that produces time-varying signals through analog or mixed-signal dynamics; an observation subsystem that measures those signals and extracts features characterizing the device's current behavior; a policy engine that evaluates contextual conditions associated with the

requested blockchain operation; and a message-physics binding mechanism that generates an authorization artifact coupling the canonical operation message to the device's verified physical state at the moment of approval.

The complete hardware and software environment responsible for these steps is referred to here as the authorization appliance. The authorization device is the hardware element within that appliance that performs physical-state verification and artifact generation. The physical module is the signal-generating subsystem within the device. The resulting authorization artifact is the evidence object that accompanies a privileged blockchain transaction.

When a privileged operation is requested, the system first verifies that the authorization device remains within its enrolled region. It then evaluates whether the requested action satisfies the relevant operational rules, such as governance approval thresholds, collateral conditions, transaction sequencing requirements, or release constraints. If both conditions hold, the message-physics binding mechanism generates an authorization artifact associated with the canonical message to be executed. Verification logic then confirms the message-artifact relationship before the privileged action is allowed to proceed.

In plain terms, the workflow is straightforward: observe the device, verify its physical state, evaluate policy conditions, bind the approved message to the measured state, and authorize only if all required conditions hold.

The remainder of the paper moves from problem to mechanism, and then from mechanism to security, implementation, and implications. Section 3 shows where the control-plane weakness appears in practice. Section 4 describes the architecture in detail. Sections 5 and 6 formalize and analyze the model. Sections 7 through 10 compare the approach with existing security architectures and examine implementation, use-case, and policy consequences. Section 11 identifies the most important future research directions.

3. The Cryptocurrency Control-Plane Security Problem

Modern cryptocurrency ecosystems rely on a wide range of operations that extend beyond the basic transaction-validation mechanisms provided by blockchain consensus protocols. While the consensus layer ensures that transactions recorded on the ledger are cryptographically valid and globally consistent, many of the most consequential actions within a blockchain system originate from privileged operational mechanisms responsible for managing the system itself. These operations can alter the economic state, operational structure, or trust assumptions of the network, and they therefore require explicit approval mechanisms operating outside the ordinary consensus path [4], [5].

The recurring problem is not that consensus fails to validate transactions correctly. It is that the authorization pathway for privileged transactions can be compromised before the transaction ever reaches consensus. When that happens, the blockchain may faithfully

execute an instruction that is syntactically valid and cryptographically well formed, but operationally illegitimate.

In practice, these control-plane functions are typically implemented through administrative signing authority, validator credentials, distributed key-management systems, or related digital authorization constructs. Although these approaches can be effective when properly managed, they introduce vulnerabilities arising from the operational environments in which authorization credentials are stored, transmitted, approved, and used. Each of the following examples reflects the same structural weakness: final authority for a high-impact action remains too easily separable from the real conditions under which that action ought to be approved.

3.1 Stablecoin Issuance Systems

Stablecoin issuers and related tokenized-asset systems often control minting and burning through privileged authorization workflows tied to collateral, reserves, or administrative policy. These are not merely routine transactions; they are supply-changing operations with direct economic consequences. Unauthorized issuance can undermine system integrity even if every on-chain step is otherwise processed correctly [6].

In many deployed systems, the final authority to change supply still depends on a limited set of private keys or governance-controlled credentials. Hardware protection and multi-signature controls can improve security, but they do not eliminate the underlying reliance on reusable digital authority. If that authority is compromised, an attacker may initiate supply changes without violating consensus rules [6], [10]. Incidents such as the Beanstalk governance attack illustrate how control over authorization pathways can be leveraged to produce economically damaging outcomes even while the underlying blockchain continues to function as designed [6].

3.2 Cross-Chain Bridge Infrastructure

Cross-chain bridges enable assets to move between independent blockchain networks by locking value on one chain and authorizing corresponding release or issuance on another. Because bridge contracts often control large pools of locked assets, the integrity of release authorization is critical [7], [8].

Many bridge systems rely on validator committees, relayers, or signing arrangements that observe events on one chain and approve actions on another. The security of the bridge therefore depends not only on smart-contract logic, but also on the integrity of the credentials and operational infrastructure behind the release decision. When attackers compromise those credentials or the environments used to manage them, they can trigger unauthorized releases even though the underlying chains continue to function as designed [7], [8]. The Ronin Bridge compromise is emblematic of this pattern: the decisive failure was not consensus itself, but validator-side authorization compromise [8].

3.3 Governance Upgrade Mechanisms

Governance systems allow communities or designated stakeholders to change protocol behavior through voting and execution workflows. Proposals may introduce new smart-contract logic, modify protocol parameters, or authorize treasury actions. Even where proposal formation and voting are decentralized, the final implementation step often depends on a privileged execution path [9].

That execution path creates a distinct risk surface. If the credentials or infrastructure used to carry out approved changes are compromised, malicious upgrades or treasury actions may be executed under the appearance of formal legitimacy [6], [9]. Governance-related attacks have shown that control over the authorization pathway for execution can sometimes be more consequential than attacks against the protocol's ordinary transaction-validation logic.

3.4 Institutional Custody Infrastructure

Institutional custody platforms use layered approval processes, multi-party controls, and specialized hardware to protect large asset balances. Yet the authority to move funds still typically reduces to the ability to produce valid signatures through an approved operational workflow [10].

As a result, attackers often target the surrounding environment rather than the blockchain or cryptographic primitive itself. Administrative systems, relay infrastructure, internal tooling, and human approval pathways become attractive compromise points because they can be used to induce valid-looking but unauthorized transfers [10]. Numerous exchange and custody breaches have followed this general pattern: the attack succeeds not by defeating the blockchain's cryptography, but by compromising the systems and workflows through which authorization is exercised.

3.5 Structural Implications for Cryptocurrency Security

Across stablecoin issuance, bridge release, governance execution, and custody transfer, the same structural lesson appears: control-plane security is often limited by how privileged authorization is represented and exercised. A cryptographic signature can prove that an action was issued through a recognized credential. It does not, by itself, prove that the action was approved under the correct physical, operational, or policy conditions.

This is the deeper limitation exposed by many large-scale cryptocurrency incidents. Some of the ecosystem's most damaging failures have originated not from failure of blockchain consensus itself, but from failure of the authorization mechanisms that govern privileged operations [5]. The architecture proposed in this paper addresses that gap by coupling authorization to verified hardware behavior and explicit policy evaluation. Its goal is not to claim that privileged operations become impossible to attack. Its goal is to make approval materially harder to extract from its intended context by replacing broadly portable authority with authorization tied to verified physical state and defined operational conditions.

4. Architecture of Physical-Layer Cryptographic Authorization

4.1 Nonlinear Physical Module

At the foundation of the architecture is a physical module designed to generate complex time-varying signals through nonlinear analog or mixed-signal behavior. Unlike a conventional cryptographic accelerator, this module is not primarily a deterministic computation engine. It is a live physical system whose output reflects both circuit dynamics and real device characteristics (Figure 2).

The device may be implemented using nonlinear analog circuitry, mixed-signal architectures, or other physical mechanisms capable of producing high-dimensional time-varying signals. Its behavior may depend on factors such as nonlinear feedback, phase interactions, parasitic effects, device mismatch, noise processes, thermal conditions, and other physical influences. The result is a continuously evolving signal environment whose detailed behavior is specific to the device and its operating context.

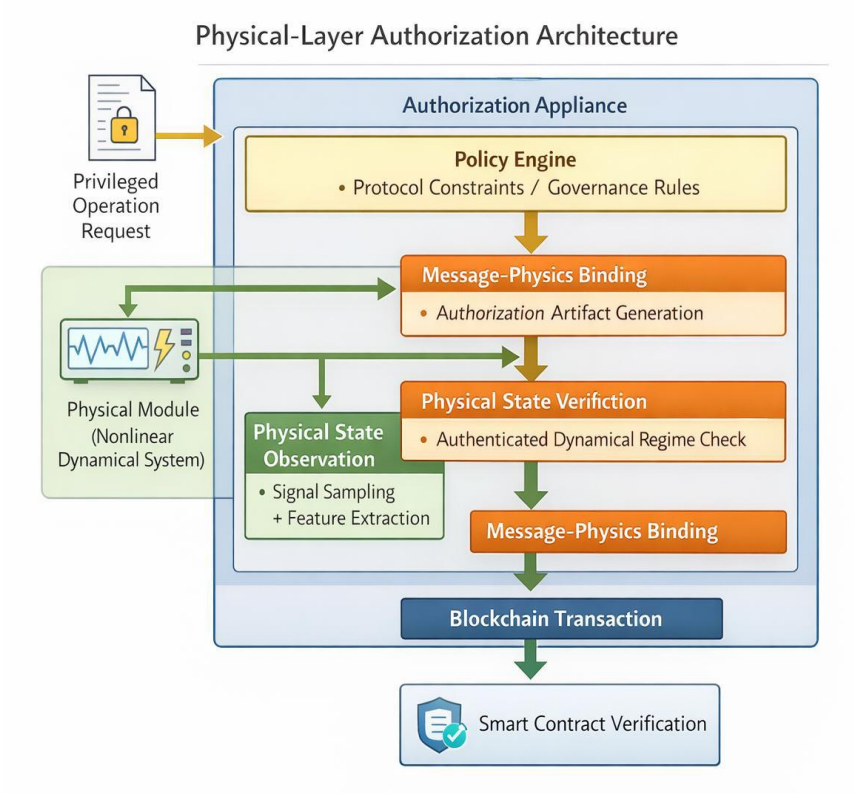


Figure 2. Physical-layer authorization architecture showing policy evaluation, physical-state observation, state verification, message-physics binding, and smart-contract verification.

Such signals may include oscillatory behavior, noise-driven fluctuations, phase-related relationships across channels, and nonlinear interactions across frequency bands. Because the system's behavior arises from real physical processes rather than purely deterministic algorithms, the exact waveform characteristics depend on both intrinsic device properties and operating conditions. The physical module therefore functions not as a static identifier or simple randomness source, but as a generator of time-varying physical behavior that can be observed and verified.

4.2 Physical State Observation and Feature Extraction

An observation subsystem measures the module's outputs and converts them into representations suitable for verification. This typically includes signal acquisition hardware together with processing steps that extract features describing the system's current behavior rather than merely recording raw waveforms.

Representative features may include spectral structure, phase relationships, entropy-related measures, temporal continuity, autocorrelation behavior, cross-channel dependencies, and other observables that capture the device's dynamical condition. Feature extraction maps measured signals into a multidimensional representation of present state. Each resulting feature vector corresponds to a particular configuration of the device's physical behavior at a specific moment in time.

Because the signals evolve continuously, the device traces a trajectory through this feature space during operation. The structure of that trajectory reflects the underlying physics of the system and forms the basis for later verification.

4.3 Enrollment and Reference Model Construction

Before the device can be trusted for authorization, it undergoes enrollment under trusted conditions. During this phase, the system observes the device over time and constructs a reference model describing the range of physical behavior associated with legitimate operation.

The enrolled model is not a single fixed fingerprint. Instead, it defines a bounded region within feature space corresponding to acceptable device behavior. That region may be established using statistical bounds, probabilistic models, or other techniques capable of representing lawful variability across multidimensional observations.

The enrollment process must account for natural variation caused by factors such as temperature change, supply fluctuation, calibration effects, aging, and ordinary environmental drift. The resulting enrolled region defines the range of physical behavior that the system treats as consistent with legitimate device operation.

4.4 Runtime State Verification

During normal operation, the observation subsystem continually or periodically evaluates the device against the enrolled region. If the extracted feature vector falls within that region, the device is treated as being in a verified physical state. If the observed behavior departs materially from the enrolled region, the authorization path is disabled or suspended pending recovery, revalidation, or other operator-defined handling.

Such deviations may arise from hardware malfunction, environmental disturbance, signal injection attempts, or physical tampering. Because the verification process evaluates multidimensional dynamical features rather than simple signal values, reproducing the expected behavior through emulation or injection is materially more difficult than merely replaying a captured credential.

This step is central to the architecture because possession of hardware is not enough. The system requires the authorization device to be present and behaving as expected at the time authorization is requested.

4.5 Protocol-Aware Authorization Policy

Physical integrity alone is not enough. Privileged blockchain operations must also satisfy the rules governing the system in which they are being requested. The architecture therefore includes a policy engine that evaluates contextual inputs from blockchain nodes, governance processes, oracle feeds, operational databases, and other relevant sources.

For stablecoin issuance, the policy engine may check reserve and collateral conditions. For bridge release, it may verify source-chain events and finality. For governance execution, it may confirm voting thresholds, timelocks, and upgrade parameters. Authorization proceeds only when the policy conditions for the requested action are satisfied.

4.6 Canonical Message Construction

Once the request passes physical verification and policy review, the system constructs a canonical representation of the operation to be authorized. This canonical message includes the information necessary to make the requested action deterministic and unambiguous, including operation type, destination contracts or accounts, parameters, nonces, time limits, and other replay-control fields.

Canonicalization matters because the authorization artifact must correspond to a well-defined operation and not merely to a loosely described approval event. The canonical message therefore serves as the formal description of the operation that the authorization mechanism approves.

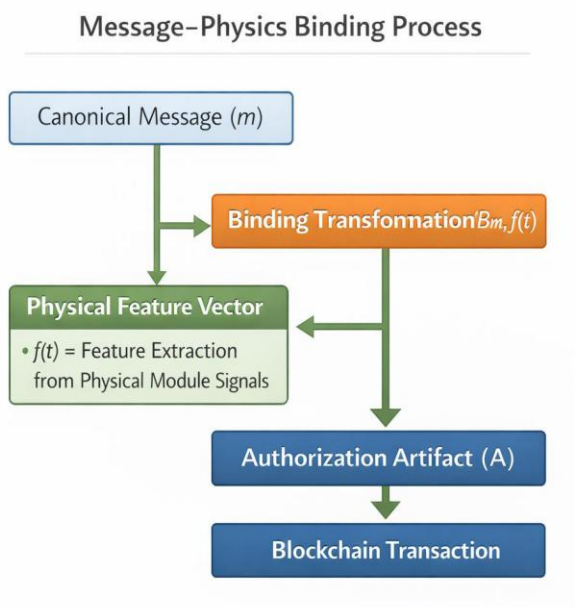


Figure 3. Message-physics binding process coupling a canonical message with the physical feature vector to generate an authorization

4.7 Message-Physics Binding

The final stage binds the canonical message to the device's present physical state. Instead of producing a conventional signature from a stored private key, the system generates an authorization artifact from a transformation that incorporates both the operation message and features derived from the device's verified real-time behavior. Through this binding process, authorization becomes inseparable from the real-time behavior of the authorization device. The message-physics binding concept is illustrated in Figure 3.

Because the device's physical state evolves over time, the resulting artifact is linked to a specific authorization event rather than to a persistent reusable credential. Even if the same message were presented again later, the resulting artifact would differ because the device's state would have changed. Capturing an

artifact therefore does not yield a portable authority token that can simply be replayed later or transplanted into a different operating environment.

5. Formal System Model

A formal model helps clarify the authorization condition implemented by the architecture and the security logic that follows from it. The purpose of this section is not to convert the paper into a mathematical treatment, but to state more precisely what must be true before a privileged authorization artifact is produced.

The nonlinear physical module described in Section 4 can be modeled as a stochastic dynamical system whose internal state evolves over time under the influence of both deterministic circuit dynamics and stochastic physical processes. Let x(t) denote the internal physical state of the authorization device at time t. This state may encompass electrical quantities such as voltages, currents, phase relationships, and other internal device characteristics, together with stochastic influences such as thermal noise and environmental fluctuation.

Because the full internal state is not directly observable, the system measures a set of signals s(t) generated by the device. These signals are processed through a feature extraction transformation that maps the raw observations into a lower-dimensional representation describing the device's present behavior. Let f(t) denote the resulting feature vector.

Each feature vector corresponds to a point in a multidimensional feature space representing the device's instantaneous state. As the device operates, the sequence of feature vectors forms a trajectory through that space. During enrollment, trusted observations are used to construct a reference model defining an enrolled region *R* corresponding to acceptable physical behavior. Because real hardware systems exhibit lawful variability due to environmental conditions, calibration effects, and aging, the enrolled region is treated as a bounded set rather than as a single fixed point.

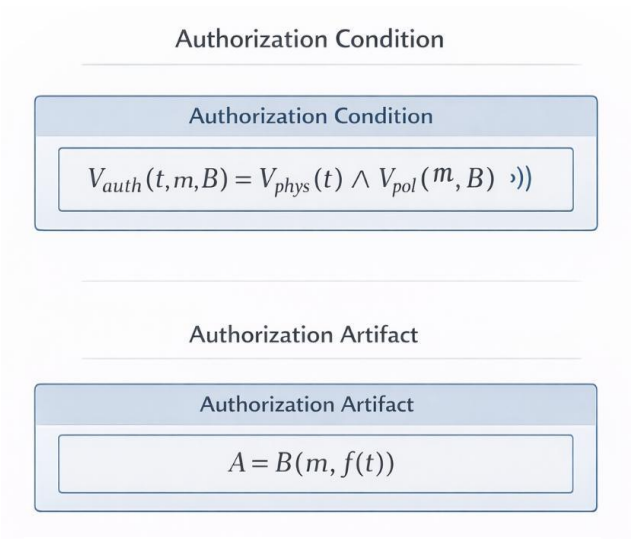


Chart 1. Formal authorization model summarizing the authorization condition and authorization artifact relationship.

The formal authorization model is summarized in Chart 1

At runtime, the system evaluates a physical verification predicate $V_{phys}(t)$, which is true when the observed feature vector lies within the enrolled region *R*. In parallel, let *m* denote the canonical message describing the requested blockchain action, and let *B* denote the relevant blockchain and policy context. A policy predicate $V_{pol}(m, B)$ is true only when the requested action satisfies the applicable protocol and operational rules.

Authorization occurs only when both predicates are true. In simplified form, the authorization condition may be expressed as the conjunction of physical verification and policy verification. If either predicate fails, the system refuses to generate an authorization artifact.

When both conditions hold, the system produces an artifact $A = T(m, f(t))$, where T represents the message-physics transformation binding the canonical operation message to the feature representation of the current verified device state. From the perspective of the blockchain system, the artifact functions analogously to a message-specific authorization object accompanying the canonical operation message. Unlike a conventional signature, however, it does not originate from a persistent private key. Instead, it reflects the device's verified physical state at the time approval is granted.

The formal model therefore captures the system's central security principle: privileged authorization is produced only when the device is in a verified physical state, the requested action satisfies policy, and the resulting artifact is bound to that specific approved message and moment of operation. In this sense, authorization artifacts correspond to transient physical approval events tied to device state and message context rather than to reusable digital credentials.

6. Adversary Model and Security Analysis

6.1 Security Objectives

The architecture is designed to support several security properties relevant to privileged blockchain operations. These objectives describe the conditions under which authorization artifacts may be generated and the protections the authorization path is intended to provide. They should be understood as architectural goals whose realized strength in deployment depends on implementation quality, feature design, enrollment robustness, verification thresholds, operational controls, and the specific binding transformation employed.

Unforgeability.

No adversary lacking access to an authorization device in a verified physical state should be able to generate a valid authorization artifact for an arbitrary canonical message. The privileged authorization path is therefore designed so that artifact generation cannot be reduced to software emulation or to compromise of surrounding operational infrastructure alone.

Replay Resistance.

Authorization artifacts are bound both to the canonical message describing the requested action and to the device's physical state at the time approval is granted. Because canonical messages may include nonce and validity constraints, and because the device state evolves over time, captured artifacts are intended to be substantially more difficult to reuse outside their original approval context.

Device-Bound Authorization.

Authorization artifacts are intended to be inseparable from the authorization device that produced them. The binding transformation incorporates features derived from the device's real-time physical behavior, so that authorization cannot be reproduced outside the hardware environment responsible for generating the artifact.

Policy-Constrained Authorization.

Authorization artifacts are generated only when both physical-state verification and policy evaluation succeed. Privileged blockchain operations may therefore be approved only when the authorization device is in a verified physical state and the requested action satisfies the policy conditions governing the system.

6.2 Adversary Model

The adversary model characterizes the capabilities of attackers interacting with the system and evaluates the architecture under realistic threat conditions. Cryptocurrency infrastructure operates in a highly adversarial environment in which attackers may possess substantial computational resources, detailed architectural knowledge, and the ability to compromise surrounding operational infrastructure.

The adversary is assumed to have full visibility into the blockchain network and may observe or record authorization transactions transmitted to the network. The adversary may also attempt to compromise software systems surrounding the authorization device, including transaction relay infrastructure, administrative interfaces, monitoring systems, or internal approval workflows. In addition, the adversary may attempt to emulate the behavior of the authorization hardware by constructing devices or algorithms designed to generate signals resembling those produced by the legitimate system.

In stronger threat scenarios, the adversary may also attempt physical attacks against the authorization device itself, including probing, power manipulation, signal injection, or attempts to infer or reproduce device behavior from observed measurements. Such capabilities reflect realistic threat models for hardware deployed in high-value financial infrastructure.

The model does not assume that an attacker can perfectly replicate the device's real-time nonlinear physical behavior with sufficient fidelity to satisfy state verification under the legitimate system's thresholds. The architecture's security value depends in part on making such replication materially more difficult than compromise of a traditional digital signing path.

6.3 Representative Attack Analyses

The following analyses are representative rather than exhaustive and are intended to show how the architecture changes the attack surface relative to conventional key-based authorization paths.

6.3.1 Resistance to Key Extraction Attacks

Traditional key-based systems concentrate reusable authority in a digital secret. If that secret is extracted or misused, arbitrary approved-looking messages can be generated. In the proposed architecture, there is no single persistent signing key playing that role in the privileged authorization path. Compromising surrounding infrastructure does not, by itself, produce the live verified physical condition required for artifact generation.

6.3.2 Replay Attack Mitigation

Replay is constrained through both message construction and physical binding. Canonical messages can include nonces, validity windows, sequence controls, and other replay-limiting fields, while the artifact also depends on the device's current measured state. That combination is intended to make artifact reuse outside the original approval context substantially more difficult.

6.3.3 Infrastructure Compromise

If an attacker compromises administrative systems, relay components, or monitoring infrastructure, the attacker may be able to submit malicious requests. The architecture is designed to ensure that such requests are still blocked unless they satisfy both policy evaluation and physical-state verification. In other words, surrounding-system compromise does not automatically transfer final authority.

6.3.4 Signal Emulation and Modeling Attacks

An advanced adversary may try to synthesize outputs that resemble the device's observed signals. The difficulty of doing so depends on the richness of the chosen observables, the quality of the enrolled model, and the temporal demands of the binding process. By requiring consistency with a live multidimensional physical trajectory rather than with a static secret, the architecture is designed to raise the bar for real-time emulation and modeling.

6.3.5 Physical Tampering

Physical manipulation of the device may alter its statistical or dynamical behavior in detectable ways. If such changes push the observed state outside the enrolled region, the authorization path fails closed. This does not eliminate the need for physical hardening, but it gives the architecture a direct behavioral mechanism for detecting and responding to certain forms of tampering.

6.3.6 Overall Security Implication

Taken together, these properties shift the attack problem from stealing or coercing one reusable digital credential to defeating several linked conditions: verified physical state, accepted policy state, and correct message-specific binding at the moment of approval.

7. Comparison with Existing Security Architectures

The proposed architecture does not render existing security technologies obsolete, and in many deployments it may complement them. Instead, it addresses a different question: whether privileged blockchain authority must ultimately reduce to possession of a digital secret. The comparisons below clarify that distinction by showing how the proposed model differs from several widely used security technologies.

Table 1 compares the proposed architecture with existing security technologies.

Security Model Comparison

Architecture	Authorization Source	Attack Target
HSM	Private Key	Key extraction
TEE	Enclave Key	Software / enclave attack
MPC	Distributed key shares	Node compromise
PUF	Challenge–response mapping	Modeling attacks
Physical Authorization	Real-time physical dynamics	Device presence + verified state

Table 1. Security-model comparison across HSM, TEE, MPC, PUF, and physical authorization architectures.

7.1 Hardware Security Modules

Hardware security modules protect private keys against extraction and can enforce important operational controls. In an HSM-based architecture, signing authority remains rooted in a protected but reusable cryptographic credential. This approach provides strong protection against direct key extraction attacks and is widely used in financial systems and cryptocurrency custody platforms [11].

Its limitation, in the present context, is that the HSM still authorizes by applying that protected signing credential when it receives a request through an approved workflow. If malicious requests reach the HSM through compromised infrastructure, administrative credentials, or software vulnerabilities, the HSM may still produce valid signatures because it has no independent knowledge of whether the broader operational context is legitimate. The physical-layer architecture differs by requiring both a verified physical state and policy compliance at the moment authorization is issued [11].

7.2 Trusted Execution Environments

Trusted execution environments isolate sensitive code and data within protected processor contexts. They can reduce exposure of stored keys and critical computations by executing them inside protected enclaves or secure processor regions [12].

However, TEEs remain fundamentally digital systems whose security depends on enclave integrity, software correctness, and memory protection. Attacks against enclave implementations, side-channel leakage, or trusted software flaws may still expose secrets or enable unauthorized operations. The proposed architecture shifts the root of authority away from protected memory and toward externally verifiable real-time physical behavior [12]. In

that sense, it relies on a different trust foundation: not secrecy of enclave state, but verification of device behavior at the time approval is granted.

7.3 Multi-Party Computation

MPC systems distribute signing authority across multiple participants so that no single actor controls the full key. This can materially improve operational resilience and reduce the risk associated with single-point compromise. MPC is therefore a meaningful improvement over simpler custody models and is especially relevant in institutional environments [10], [13].

Yet the resulting authority is still key-based authority reconstructed through a distributed protocol. If an attacker compromises a sufficient number of participants, or successfully interferes with the operational environment supporting the protocol, the signing authority may still be used to authorize transactions. By contrast, the architecture proposed here removes the need for a reconstructable control-plane key and can instead require one or more independent device-bound authorization events [10], [13].

7.4 Physical Unclonable Functions

PUFs show how manufacturing variation can be used for device-specific security behavior. In many implementations, they are used for challenge-response functions, device identification, or derivation of cryptographic keys without explicit long-term key storage [14], [15].

The present architecture differs in a more specific way. It does not rely on a discrete challenge-response mapping or a quasi-static device-specific output. Instead, it relies on continuously evolving physical dynamics and ongoing behavioral verification rather than on a fixed or quasi-fixed response mapping [14], [15]. Authorization therefore depends not on reproducing one expected response, but on remaining within an acceptable region of observed time-varying behavior.

7.5 Summary of Architectural Differences

HSMs, TEEs, MPC, and PUF-based approaches each strengthen hardware or cryptographic trust in important ways, and they may remain valuable components of a broader deployment. The distinctive feature of physical-layer cryptographic authorization is narrower and more specific: it relocates privileged authority from a stored or reconstructable digital secret to a verified real-time physical condition under explicit policy control.

In that respect, the architecture is not simply another way to protect a key. It is an attempt to reduce the extent to which privileged control-plane authority depends on any portable or reconstructable credential at all.

8. System Implementation and Blockchain Integration

The architecture described in previous sections establishes the functional components required for physical-layer authorization. Practical deployment requires integrating those components with existing blockchain infrastructure in a manner that preserves compatibility with current protocols while strengthening control-plane security.

A practical deployment does not require altering blockchain consensus. Instead, the authorization system can be implemented as an external control-plane appliance positioned between privileged operational workflows and the transactions ultimately submitted to the network.

In a representative deployment, the system comprises three interacting layers: the authorization appliance, a blockchain observation layer, and an on-chain or associated verification layer. The appliance is responsible for physical-state verification, policy evaluation, canonicalization, and artifact generation. The observation layer provides the external state required for policy decisions. The verification layer checks the resulting authorization artifact before a privileged action is executed.

The end-to-end authorization workflow is illustrated in Figure 4.

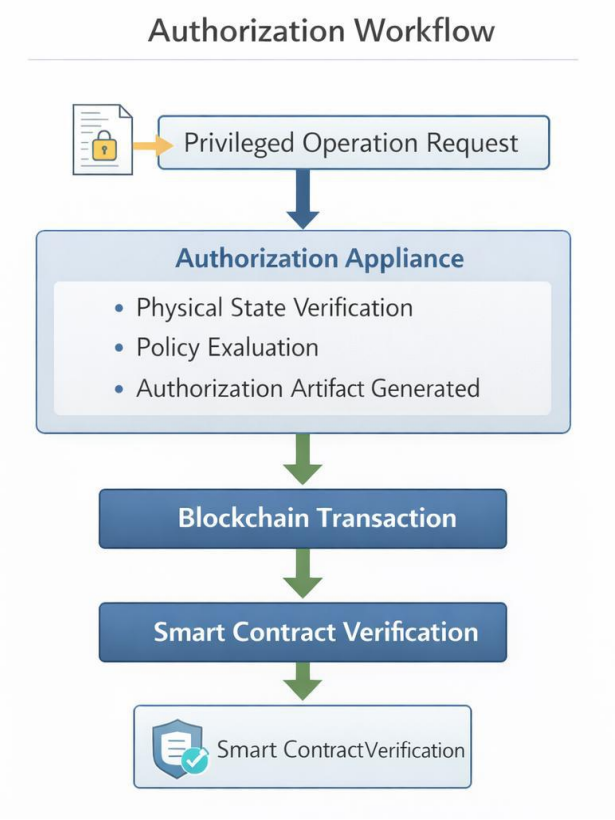


Figure 4. End-to-end authorization workflow from privileged operation request through authorization appliance, blockchain

Operationally, the sequence is straightforward. First, a privileged request is submitted to the appliance. Second, the appliance determines whether the authorization device is in a verified physical state. Third, it evaluates whether the requested action satisfies the applicable blockchain and policy conditions. Fourth, it canonicalizes the approved operation message. Fifth, it generates an authorization artifact bound to that message and the measured device state. Sixth, the resulting transaction is submitted through conventional network infrastructure. Seventh, verification logic confirms the message-artifact relationship and associated freshness controls before the privileged action is allowed to execute.

Implementation quality depends heavily on edge-case handling. The system should define clear behavior for hardware faults, uncertain measurements, stale observation data, blockchain node disagreement, chain reorganizations, communication failures, and

policy-source inconsistencies. In high-value deployments, the preferred failure mode is conservative: suspend authorization until the state of the device, the observation layer, and the policy context can be trusted again.

On-chain or near-chain verification logic should validate not only the artifact itself but also its associated replay controls, validity windows, and operation-specific constraints. This ensures that physical authorization functions as a meaningful approval gate rather than as a detached side signal.

8.1 Authorization Appliance

The authorization appliance hosts the physical device, observation subsystem, state-verification logic, policy engine, and artifact-generation path. In production settings, this environment should be designed for controlled operation, monitored state transitions, clear audit logging, and fail-safe behavior under uncertain conditions.

When a privileged operation request is received, the appliance evaluates both device state and policy context before authorization is allowed to proceed. If those conditions are satisfied, the appliance generates the authorization artifact associated with the canonical message to be executed.

8.2 Blockchain Observation Layer

Because policy evaluation depends on external blockchain facts, the observation layer should obtain state from appropriately trusted sources, ideally including multiple independent nodes where failure consequences justify the added rigor. For multi-chain operations, the appliance may need synchronized visibility into more than one network at once [16], [17].

The observation layer provides the policy engine with the information necessary to determine whether proposed operations comply with protocol rules, governance conditions, and other operational constraints.

8.3 Authorization Transaction Construction

The approved transaction should carry a deterministic message representation and the associated authorization artifact in whatever form the target blockchain system can verify. The exact encoding is implementation-dependent, but the design objective remains constant: the privileged operation should be executable only when the verified message-artifact pairing is present, current, and valid for that specific action.

The canonical message specifies the operation to be executed, while the authorization artifact provides evidence that approval was granted under the required verified conditions.

8.4 Verification Logic

Verification may occur in smart contracts, in chain-adjacent middleware, or in other trusted execution paths depending on the deployment model. Regardless of location, the verifier should confirm correspondence between the canonical message, the artifact, and the applicable freshness or sequencing controls.

Only when verification succeeds should the privileged action be allowed to execute.

8.5 Operational Safeguards

Well-designed deployments should disable authorization under abnormal device behavior, observation uncertainty, policy ambiguity, or integrity concerns affecting the appliance itself. Logging should preserve enough detail to support audits, post-incident review, and operational accountability without turning the logging layer into a substitute source of authority.

These safeguards ensure that failures, uncertainty, or abnormal operating conditions do not result in unintended authorization events.

9. Deployment Scenarios and Operational Use Cases

The architecture can secure a range of privileged blockchain functions, but its value differs by use case. In each setting, the point is not merely that an artifact is generated; it is that the artifact is generated only after the particular hardware and policy conditions relevant to that operational setting have been satisfied.

Representative deployment scenarios are illustrated in Figure 5.

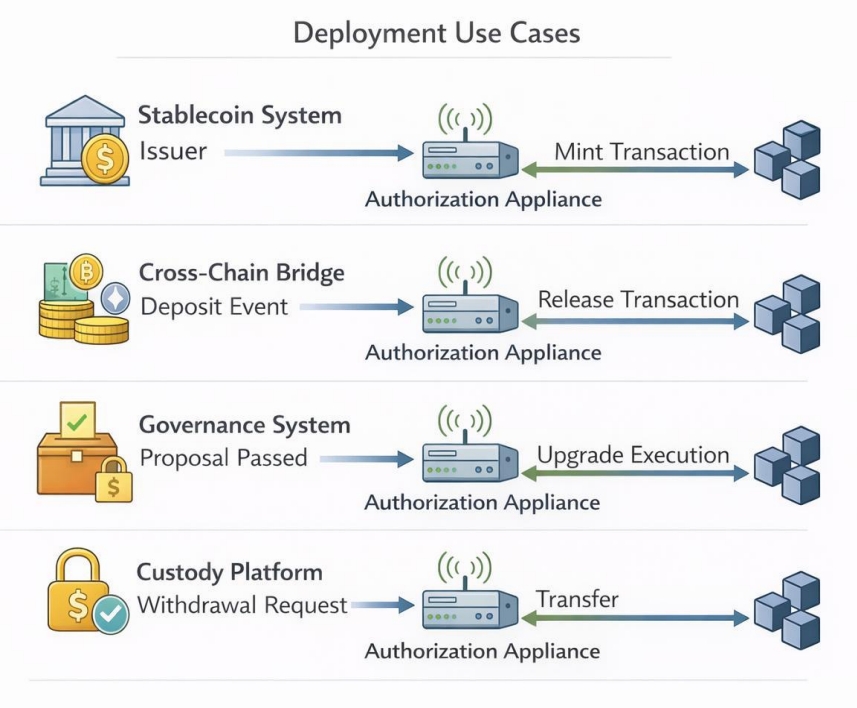


Figure 5. Deployment use cases including stablecoin issuance, cross-chain bridges, governance execution, and custody-platform transfers

9.1 Stablecoin Issuance Control

In stablecoin systems, the architecture can serve as the final control gate for minting and burning. These are supply-changing operations with direct economic consequences, and their integrity depends not only on cryptographic validity but also on whether reserve-related

and policy-related conditions have actually been satisfied.

The authorization appliance can verify collateralization conditions, reserve data, or other issuance constraints before approving the operation. Once those conditions are satisfied and the authorization device is in a verified physical state, the appliance generates the authorization artifact associated with the mint or burn transaction. The primary benefit in this setting is issuance discipline: supply-changing actions are tied to both verified policy conditions and verified hardware-rooted authorization rather than to administrative credentials alone.

9.2 Cross-Chain Bridge Security

In bridge systems, the architecture helps protect asset release decisions that depend on facts observed on another chain. Because bridge contracts often control large pools of locked value, release integrity is critical.

The authorization appliance can verify that a corresponding deposit or burn event has occurred on the source chain and that the event has reached the required finality threshold. After confirming those conditions and verifying the authorization device's physical state, the system generates the authorization artifact required for the release transaction. The primary benefit in this setting is release integrity: bridge outflows are conditioned on verified source-chain facts, policy thresholds, and live hardware-rooted authorization before destination-chain execution occurs.

9.3 Governance Upgrade Execution

For governance frameworks, the architecture can strengthen the execution path after proposal approval. Governance systems may decentralize proposal formation and voting, yet the final execution of an approved change still depends on a privileged operational path.

The authorization appliance can verify that governance requirements have been satisfied, including proposal approval status, threshold conditions, timelocks, and upgrade parameters, before approving execution. Once those conditions are confirmed and the authorization device is in a verified physical state, the appliance generates the authorization artifact associated with the upgrade or treasury action. The primary benefit in this setting is execution-path control: even when a vote passes, the actual privileged action still requires a verified authorization event tied to the approved message and current governance conditions.

9.4 Institutional Custody Transactions

In custody settings, the architecture can operate as a final approval stage after internal workflows are completed. Asset transfers, withdrawals, and settlement actions may already pass through multi-party review and internal policy checks before they are prepared for blockchain submission.

After those internal approvals are completed, the transaction request can be submitted to the authorization appliance, which verifies relevant policy constraints such as withdrawal limits, authorization thresholds, or client-specific conditions. If those conditions are satisfied and the device remains in a verified physical state, the appliance generates the artifact required for the transfer. The primary benefit in this setting is operational gating: large transfers or withdrawals become dependent on both institutional policy satisfaction and live hardware-rooted authorization rather than on administrative credentials alone.

9.5 Validator and Oracle Authorization

Validator admission, validator-role changes, and oracle updates can also be tied to the model. These are control-plane functions because they can directly affect trust, liveness, or downstream smart-contract behavior [16], [17].

Validator admission transactions may require an authorization artifact before new participants are added to the validator set. Similarly, oracle updates influencing smart contract execution may require hardware-rooted authorization before new data values are accepted by the system. The primary benefit in this setting is control-function hardening: operational changes that affect trust or execution conditions need not depend solely on possession of the right digital credential [16], [17].

9.6 Control-Plane Security Framework

Taken together, these examples show that the architecture is best understood as a control-plane hardening framework. It is most relevant where a blockchain system already has functioning consensus and cryptographic validation but still faces outsized risk from how privileged authority is operationally exercised. By requiring hardware verification and policy satisfaction to converge before authorization is produced, the framework ties high-impact blockchain actions to the verified conditions under which they are actually approved.

10. Policy Implications and Regulatory Applications

The architecture has implications beyond technical design because it changes what can be asserted about approval of high-impact blockchain actions. Instead of saying only that a transaction was signed by a recognized credential, operators may be able to say that it was approved under a defined combination of verified hardware behavior and policy conditions.

This distinction may matter to institutional operators, auditors, and regulators seeking stronger assurance around issuance controls, custody movement, governance execution, and other administrative functions in digital asset infrastructure. As digital asset systems increasingly support activities resembling traditional financial operations, including issuance, settlement, custody, and market infrastructure, the need for stronger operational assurance grows accordingly.

10.1 Verifiable Monetary Control

For token issuance systems, hardware-rooted authorization can make supply-changing actions more explicitly traceable to defined approval conditions. That does not eliminate the need for reserve audits or governance oversight, but it can make the control path for issuance materially more explicit and technically enforceable.

Because authorization artifacts accompany blockchain transactions, supply-changing actions can be linked more directly to the approval process responsible for authorizing them. This provides a clearer basis for demonstrating that issuance or redemption occurred through the intended operational pathway rather than merely through possession of a valid credential.

10.2 Transparent Operational Auditability

Because the appliance can record authorization decisions, state-verification outcomes, and policy-evaluation results, the architecture can improve visibility into why a privileged action was approved. When paired with blockchain records, this can create a more complete trail of both execution and approval.

Such auditability may be valuable for institutional oversight, regulatory reporting, and post-incident forensic review. Blockchain systems make on-chain execution visible, but they often provide limited visibility into the operational process that authorized that execution. Physical-layer authorization can narrow that gap.

10.3 Institutional Compliance Enforcement

In institution-facing environments, the architecture can help convert certain procedural requirements into technical gating conditions. Where a workflow requires approvals, thresholds, or documentary prerequisites before transfer, the authorization layer can be designed so that the privileged blockchain action cannot proceed until those conditions have been satisfied.

In that respect, the architecture can serve as a technically enforced control point within broader operational and compliance workflows, rather than as a purely cryptographic mechanism detached from institutional process.

10.4 Governance Safeguards for Protocol Upgrades

Governance systems often distinguish between proposal legitimacy and execution integrity. The proposed model adds a hardware-rooted approval step to the execution side of that equation, helping reduce the risk that technically valid but procedurally improper changes are carried out through compromised execution channels.

Policy checks may include confirmation of proposal approval, enforcement of governance delay periods, and validation of upgrade parameters. The value here is not only that

governance can approve change, but that execution of that change can be tied to a more controlled and verifiable authorization path.

10.5 Adjacent Relevance to CBDC and Regulated Digital Money

Although this paper focuses on cryptocurrency infrastructure, the same control principles may be relevant to central bank digital currency systems or other highly regulated digital-money environments where issuance, settlement, or emergency administrative actions require especially strong operational assurance.

This is best understood as adjacent relevance rather than a central claim of the paper. The point is that any digital monetary system with high-consequence administrative actions may benefit from stronger coupling between operational approval conditions and the mechanism that authorizes execution.

10.6 Policy Perspective on Hardware-Rooted Authority

From a policy standpoint, the key significance of the architecture is the move from credential possession to controlled hardware-rooted authorization for especially sensitive operations. Traditional digital security models rely on protecting secrets whose compromise can transfer authority to an unauthorized actor. By contrast, the architecture described here ties authorization to the verified behavior of a specific physical system operating under defined policy constraints.

This model aligns more closely with security practices used in critical financial and infrastructure systems, where sensitive operations are often tied to controlled hardware environments and procedural verification mechanisms. In that sense, the architecture offers a path toward digital asset systems that preserve blockchain transparency while adding stronger operational discipline at the points where institutional or administrative authority is actually exercised.

11. Future Research Directions

The most important research agenda can be grouped into four areas: formal security foundations, hardware and signal engineering, distributed deployment and attestation, and applications beyond cryptocurrency. Together, these directions define the path from architectural concept to deployable high-assurance authorization framework.

11.1 Formal Security Foundations

Future work should develop rigorous security definitions for message-physics binding, artifact unforgeability, replay resistance, and resistance to modeling or adaptive emulation. Formal treatment would help distinguish claims that follow from architecture alone from claims that depend on specific implementation choices.

One important direction is to model the authorization device as a stochastic dynamical system whose observable outputs contribute to the binding transformation under explicit security assumptions. Another is to examine how this framework can coexist with evolving cryptographic standards, including post-quantum primitives, so that both the physical and mathematical components of the authorization path remain resilient over time.

11.2 Hardware and Signal Engineering

Further research is needed on physical module design, observable selection, enrollment methodology, verification thresholds, environmental robustness, drift management, and tamper-aware operating envelopes. The practical strength of the architecture will depend heavily on how these engineering questions are answered.

This includes balancing two competing requirements: generating sufficiently rich physical dynamics to resist emulation or modeling, while maintaining behavior stable enough to verify within a defined enrolled region. Future work may draw on nonlinear circuits, hybrid analog-digital architectures, advanced signal analysis, and adaptive reference-modeling techniques capable of distinguishing lawful drift from attack-induced deviation.

11.3 Distributed Deployment and Attestation

Higher-assurance deployments may require multiple independent authorization devices, remote attestation of approved hardware, artifact aggregation methods, and protocols for coordinating device-bound approvals across different trust domains or geographic locations [18].

In such systems, privileged actions could require convergence of multiple independently verified authorization events rather than reliance on a single approval source. Research in this area may therefore focus on fault tolerance, resilience under partial compromise, remote hardware trust establishment, and governance of approved-device registries.

11.4 Applications Beyond Cryptocurrency

The underlying concept may also apply to other domains in which a small number of high-value digital actions require stronger authorization assurance than portable credentials alone can provide, including financial infrastructure, industrial control, secure data access, and selected digital identity systems.

The broader implication is that physical-layer authorization may represent more than a cryptocurrency-specific control mechanism. It may point toward a wider security model in which critical digital actions are authorized not merely by possession of a secret, but by demonstration of verified physical behavior under defined operating conditions.

Taken together, these research directions suggest a broader shift toward hardware-rooted digital authority. Continued work will determine how physical-layer authorization can

complement existing cryptographic methods and contribute to more resilient security architectures in blockchain infrastructure and beyond.

12. Conclusion

The central security problem addressed in this paper is not failure of blockchain consensus. It is the continued reliance of privileged cryptocurrency operations on authorization mechanisms that ultimately reduce to portable digital credentials. That design leaves critical control-plane functions exposed to theft, coercion, misuse, and operational compromise even when the underlying ledger behaves correctly.

The architecture presented here offers a different model. Instead of deriving privileged authority from a persistent digital secret, it ties authorization to the verified real-time physical behavior of a dedicated device operating under explicit policy constraints. In that model, authority is not something merely possessed; it is something demonstrated under controlled conditions at the time approval is granted.

This shift has practical significance for stablecoin issuance, cross-chain release, governance execution, validator and oracle control, and institutional custody. It also has broader conceptual significance: it suggests that some forms of digital authority, especially those governing high-consequence operational actions, may be better secured when they are rooted in verified physical processes rather than in reusable digital secrets.

The proposed framework also preserves compatibility with existing blockchain environments. By functioning as an overlay authorization layer rather than as a replacement for consensus, it offers a path for strengthening control-plane security without requiring fundamental redesign of the underlying network.

As digital asset infrastructure continues to mature, the pressure to strengthen control-plane assurance will increase. Physical-layer cryptographic authorization offers one possible path: preserve the advantages of existing blockchain systems while hardening the operational boundary where privileged authority is actually exercised. More broadly, it suggests a direction for digital financial infrastructure in which authorization is grounded not only in cryptographic mathematics, but also in verifiable physical conditions.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," 2013.

[3] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," NIST Interagency/Internal Report (NISTIR) 8202, Oct. 2018.

[4] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," in Proceedings of the 4th ACM Conference on Advances in Financial Technologies, 2022.

[5] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "SoK: Decentralized Finance (DeFi) Attacks," in 2023 IEEE Symposium on Security and Privacy (SP), 2023, pp. 2444-2461.

[6] Immunefi, "Hack Analysis: Beanstalk Governance Attack," Apr. 2022.

[7] M. Zhang, X. Zhang, J. Barbee, Y. Zhang, and Z. Lin, "SoK: Security of Cross-Chain Bridges: Attack Surfaces, Defenses, and Open Problems," arXiv:2312.12573, 2023.

[8] Sky Mavis, "Sky Mavis Raises $150M Led by Binance, Funds to be Restored on the Ronin Bridge," Mar. 2022.

[9] J. Ma, M. Jiang, J. Jiang, X. Luo, Y. Hu, Y. Zhou, Q. Wang, and F. Zhang, "Understanding Security Issues in the DAO Governance Process," 2025.

[10] V. Di Nicola, R. Longo, F. Mazzone, and G. Russo, "Resilient Custody of Crypto-Assets, and Threshold Multisignatures," Mathematics, vol. 8, no. 10, art. 1773, 2020.

[11] National Institute of Standards and Technology, "FIPS 140-3: Security Requirements for Cryptographic Modules," Mar. 2019.

[12] V. Costan and S. Devadas, "Intel SGX Explained," technical report, Massachusetts Institute of Technology, 2016.

[13] Y. Lindell, "Fast Secure Two-Party ECDSA Signing," in Advances in Cryptology - CRYPTO 2017, LNCS 10402, 2017, pp. 613-644.

[14] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in Proceedings of the 44th ACM/IEEE Design Automation Conference (DAC), 2007, pp. 9-14.

[15] R. Maes and I. Verbauwhede, "Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions," in Towards Hardware-Intrinsic Security: Foundations and Practice. Springer, 2010, pp. 3-37.

[16] C. Duley, L. Gambacorta, R. Garratt, and P. Koo Wilkens, "The Oracle Problem and the Future of DeFi," BIS Bulletin No. 76, 2023.

[17] S. Ellis, A. Juels, and S. Nazarov, "ChainLink: A Decentralized Oracle Network," white paper, 2017.

[18] Trusted Computing Group, "Overview of TCG Technologies for Device Identification and Attestation," ver. 1.0, rev. 1.37, Jan. 2024.

Appendix A. Key Terms

Term	Definition
Authorization appliance	The complete hardware and software system responsible for physical-state verification, policy evaluation, and authorization artifact generation.
Authorization device	The hardware component of the appliance that performs physical-state verification and artifact generation.
Physical module	The nonlinear signal-generating subsystem that produces the dynamical signals used for verification.
Authorization artifact	The evidence object accompanying a privileged blockchain transaction, showing that approval was issued under verified conditions.
Canonical message	A deterministic representation of the blockchain operation to be authorized, including relevant parameters, nonces, time limits, and replay controls.
Message-physics binding	The process of coupling a canonical operation message to the authorization device's real-time physical state representation.
Control plane	The operational layer governing privileged blockchain actions such as issuance, bridge release, governance execution, validator admission, oracle updates, and custody transfers.

Appendix B. Implementation Checklist

Workstream	Required Control
Hardware enrollment	Create reference models for valid device dynamics across expected environmental conditions.
Runtime verification	Continuously or periodically sample physical module outputs and verify extracted features against enrolled dynamical regions.
Policy integration	Connect the authorization appliance to trusted blockchain nodes, governance systems, oracle feeds, and relevant operational data sources.
Canonicalization	Define deterministic message construction for each privileged operation type.
Artifact verification	Implement verification logic for authorization artifacts, freshness controls, and operation-specific constraints.
Fail-safe behavior	Disable or suspend authorization when hardware state, policy state, or observation confidence is invalid or uncertain.
Auditability	Maintain logs linking authorization outcomes to policy decisions and device-state verification results.