PHAROS
RESEARCH

Security Architecture of Public Blockchains: Risk and Strategy

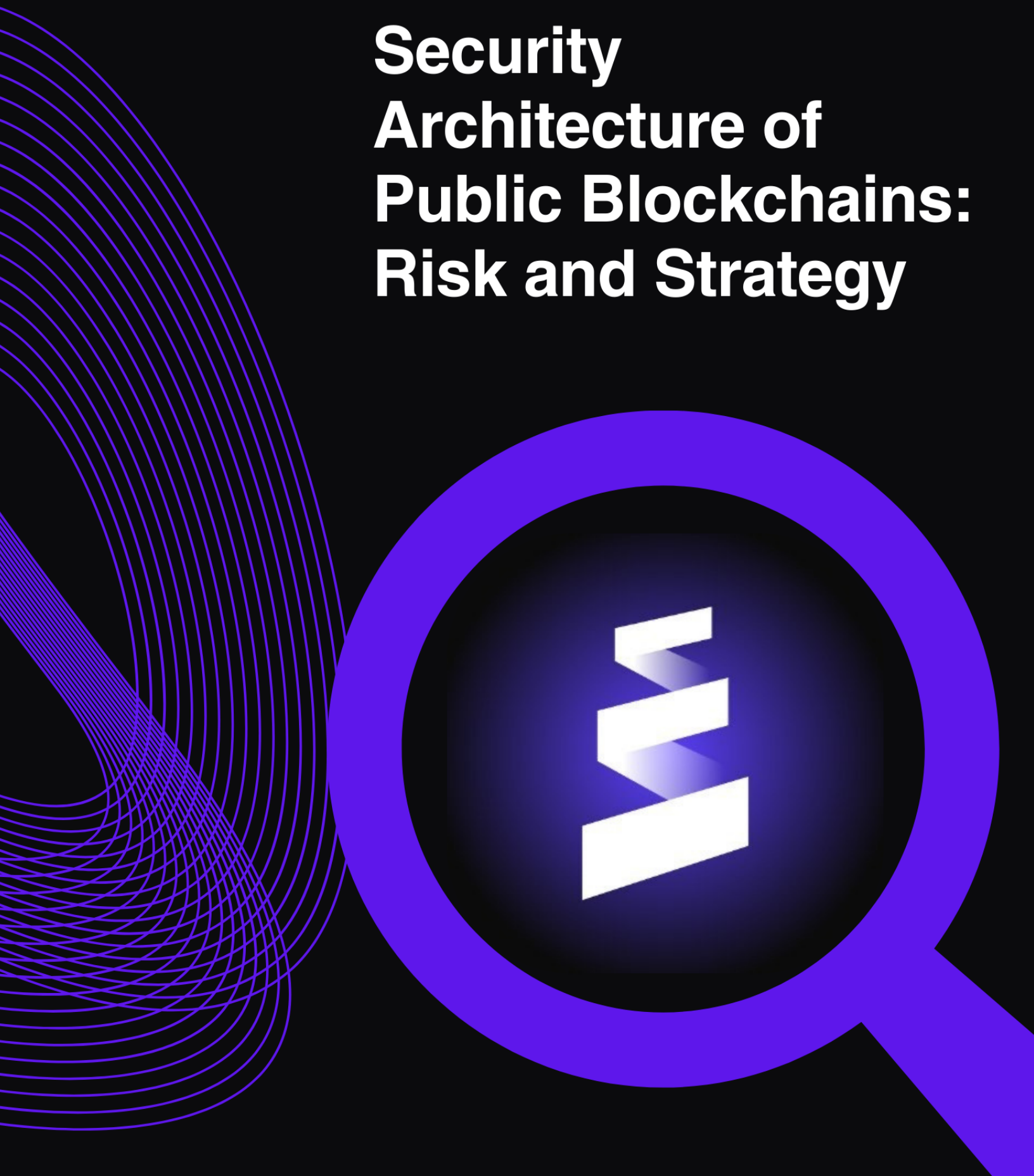


Table of Contents

01 / The Inevitability of the Evolution of Public Blockchain Security

The security of early public blockchains relied heavily on contract-centrism, with the security focus highly concentrated on the auditing of smart contract code. It was generally believed that as long as the contract itself was invulnerable, the security line would be impregnable. However, a series of costly security incidents have ruthlessly revealed the limitations of this concept. In 2023, hackers breached the control of private keys related to the airdrop distribution contract of ZKSync tokens, and assets worth millions of dollars were transferred. In June 2022, Loopring suffered a DDoS attack, and the paralysis of cloud infrastructure disrupted network services for more than ten hours. In March of the same year, North Korean hackers launched attacks targeting vulnerabilities in Ronin Bridge, an ecological partner, intruded into employees' IT infrastructure, successfully took control of four validator nodes, and directly broke through the entire defense line, making it one of the most damaging attacks in blockchain history. We can see more and more clearly that the attack surface of blockchain is no longer limited to the smart contract or virtual machine layer, but is rapidly expanding to key management, operation and maintenance infrastructure, third-party dependencies, and even social engineering attacks targeting internal personnel. The security of a blockchain system deeply depends on the real-world technology stack deployed in a complex, multi-layered manner composed of people and organizations.

This coincides with the strategic priorities of global core financial regulatory institutions such as the International Monetary Fund (IMF) and the Bank for International Settlements (BIS). In multiple speeches and reports in 2024, the IMF clearly pointed out that with the integration of crypto assets into the mainstream financial system, the focus of regulation is no longer limited to market volatility, but must be extended to deeper structural and operational dimensions, among which operational risk and governance risk are regarded as key vulnerabilities in the evolution of tokenized finance. The BIS further emphasized in multiple reports submitted to the G20 that sound governance arrangements are the cornerstone of effective risk management, and such risk management must be comprehensive and consistent throughout, covering all areas including operational risk (especially cyber resilience) and governance risk without any blind spots. These consensuses from top-level design convey a clear signal: when blockchain technology begins to carry real assets comparable to or even more liquid than those in traditional financial markets, its security standards must be in line with and seamlessly aligned with those of top financial institutions. This means that blockchain security is no longer a single link only responsible for the code level by the development team, but must evolve into a systematic project that needs to penetrate into every detail of the design of the technical architecture, the process of daily operation, the shaping of organizational culture, and the management of partners.

Against such a background, the industry needs a security model capable of carrying future digital financial assets. Such a public blockchain must possess three capabilities: responding to regulatory inquiries, carrying institutional trust, and proving that it is worthy of the trillions of value entrusted to it amid continuous real attacks. **The emergence of the Pharos public chain has timely defined the benchmark for a secure public blockchain. It takes the lead in engineering the regulatory**

frameworks of the IMF and BIS into an operable and verifiable on-chain and off-chain collaborative system, aiming to become a secure public blockchain serving trillions of real-world assets.

02 / Risk Matrix and Multi-Dimensional Architecture of Public Blockchain Security

2.1 Security Architecture of the Pharos Public Chain

Pharos is a public chain designed to serve financial institutions and high-value real-world assets (RWA). Its security architecture surpasses the common community autonomy model of public blockchains, and builds a complete guarantee system covering technology, operation, law and finance. Specifically, its security architecture fully covers the following six core dimensions to achieve certainty in public blockchain security.

First, the dimension of physical and hardware security. For financial public blockchains, the physical access control of validator nodes, key management facilities and even data centers must reach the security level of bank vaults or equivalent data centers. More importantly, certified Hardware Security Modules (HSM) are widely adopted to generate, store and process core keys, ensuring that private key materials cannot be extracted by software under any circumstances, eliminating the possibility of private key leakage from the physical root.

Second, the dimension of key management and access control. In institutional scenarios, keys represent not only control rights, but also corresponding legal ownership and responsibilities. Therefore, financial public blockchains must design a refined enterprise-level key management system, including supporting complex signature schemes such as multi-signature and Threshold Signature Scheme (TSS) to match the internal checks and balances requirements of enterprises; realizing compliant custody and recovery processes of keys to avoid permanent loss of assets caused by individual incapacity; providing role-based, auditable and fine-grained access control policies. The goal of this dimension is to securely adapt the original model of “private key equals everything” in blockchain to the strict internal governance and compliance framework of financial institutions.

Third, the dimension of network and communication security. The public blockchain network itself is an open P2P system, and financial-grade applications further require its communication to have confidentiality, integrity and high availability. This needs to be achieved by implementing a zero-trust network architecture and enforcing encryption for all communication between nodes and between clients and nodes (such as using TLS 1.3 or stronger protocols). At the same time, enterprise-level DDoS mitigation solutions must be deployed to resist traffic attacks aimed at paralyzing transaction or liquidation processes. This dimension ensures that key information such as transaction instructions and block data cannot be eavesdropped, tampered with or blocked during transmission.

Fourth, the dimension of smart contract and protocol security. Smart contract security is the traditional focus of blockchain security, and the requirements for financial public blockchains are stricter. It requires that core protocols and smart contracts (especially contracts handling asset issuance, settlement and redemption) must undergo formal verification to mathematically prove that their code behavior fully complies with design specifications and eliminate vulnerabilities such as reentrancy and overflow. In addition, a controlled contract upgrade governance process with clear rollback and emergency pause mechanisms must be established to respond to extreme situations.

For RWA assets, the contract logic must achieve accurate and tamper-proof mapping with the rights, obligations and default disposal clauses in off-chain legal documents.

Fifth, the dimension of compliance, monitoring and auditing. Financial institutions operate in a highly regulated environment, so financial public blockchains must have built-in compliance and auditability. This includes providing complete and tamper-proof audit trails of on-chain activities, and being able to integrate with off-chain monitoring, auditing and risk management systems (such as SIEM). Real-time monitoring needs to cover multiple levels such as abnormal transaction patterns, smart contract risk indicators, node health status and oracle data sources, enabling institutions to proactively detect threats, meet regulatory reporting requirements, and provide non-repudiable evidence for post-incident forensics.

Sixth, the dimension of governance, emergency response and ecological security. The ultimate security test lies in the system resilience in the face of unknown shocks. Financial public blockchains must preset a clear mechanism combining on-chain governance and off-chain emergency response, specifically including: emergency response plans for serious vulnerabilities or extreme market fluctuations; strict access, continuous evaluation and exit mechanisms for validator sets and key service providers (such as cross-chain bridges and oracles); and the transmission of security standards and collaborative defense capabilities for ecological partners (such as asset issuers and custodians). This dimension shows that security is not a static state, but a dynamic, collaborative and continuous process that can resist systemic risks through internal and external linkage.

Summary:

Figure 1: The security architecture of Pharos public chain

Security Dimension	Core Requirements	Key Technologies/Measures
1. Physical & Hardware Security	Physical access control up to bank vault level; private keys protected by hardware security modules	HSM, anti-software extraction
2. Key Management & Access Control	Enterprise-level key system, multi-signature/TSS, compliant custody and recovery, role-based access control	Multi-signature, threshold signature, role permission audit
3. Network & Communication Security	Zero trust, mandatory encryption, DDoS protection	TLS 1.3, DDoS mitigation
4. Smart Contract & Protocol Security	Formal verification, contract upgrade governance, legal mapping	Formal verification, emergency pause, legal-code mapping
5. Compliance, Monitoring & Auditing	Audit trails, real-time monitoring, SIEM integration	Tamper-proof logs, anomaly detection, regulatory reporting
6. Governance, Emergency & Ecological Security	On-chain + off-chain emergency response, access and exit, ecological collaboration	Emergency response, validator evaluation, collaborative defense

Source: Pharos Research

Summary: The Multi-Layered Security Architecture of Pharos

The security architecture represented by Pharos clearly shows that the security architecture of a financial-grade public chain starts from the trust foundation of physical hardware, penetrates every layer from keys, networks, contracts, monitoring to governance and ecology, and builds a three-dimensional, in-depth and closed-loop guarantee system. Its ultimate purpose is to transform the inherent uncertainty of blockchain technology into deterministic services that financial institutions can understand, measure and trust, thus paving the way for the secure on-chain migration of trillions of dollars in traditional assets.

2.2 Differentiation Strategy and Practical Framework

Among the six dimensions in the risk matrix, no single technical solution or operational strategy can cover all threats. A mature public blockchain security strategy must inevitably present the dual characteristics of differentiation and defense-in-depth. The essence of differentiation is that public blockchains make clear trade-offs among security, performance and decentralization according to their own positioning; while defense-in-depth is to control the impact of single-point failure within a limited range through multi-layer and complementary control measures. At present, mainstream public blockchains have gradually formed a strategic framework with both differentiated positioning and defense-in-depth characteristics, which not only provides decomposable analysis dimensions for the security path of top public blockchains, but also sets a benchmark for the security maturity evaluation of emerging public blockchains.

Technical Strategy

- The consensus layer is the first watershed of the public blockchain security foundation. Solana adopts the combination of PoH (Proof of History) + PBFT, exchanging lightweight block generation speed with high hardware thresholds, and its security assumption is anchored to the continuous leading of node computing power. In September 2025, Solana introduced the new Votor/Rotor consensus mechanism through the Alpenglow upgrade, replacing the original PoH/TowerBFT, greatly compressing the transaction finality time from about 13 seconds to 100-150 milliseconds, with a peak throughput exceeding 100,000 TPS, and supported by more than 98% of validators.[1] Ethereum adopts the hybrid PoS mechanism of Casper FFG + LMD-GHOST. At present, the number of active validators has exceeded 900,000, achieving a high level of decentralization in global distribution, with a finality time of about 12 minutes (two epochs).[2] Bitcoin's PoW anchors security in energy and special chips in the physical world, with an annual power consumption of about 175.87 TWh[3], forming a completely different computing power-as-trust model. Behind the consensus choice is the differentiated answer of public blockchains to the fundamental trade-off between security and efficiency.
- Top public blockchains have generally started the migration preparation for post-quantum cryptography and deeply integrated zero-knowledge proof technology. IACR 2025 research pointed out that blockchains adopting EdDSA and SLIP-0010 key derivation standards (such as Sui, Solana, Near, Aptos) have structural advantages in post-quantum migration – they can prove seed ownership through post-quantum zero-knowledge proofs and realize

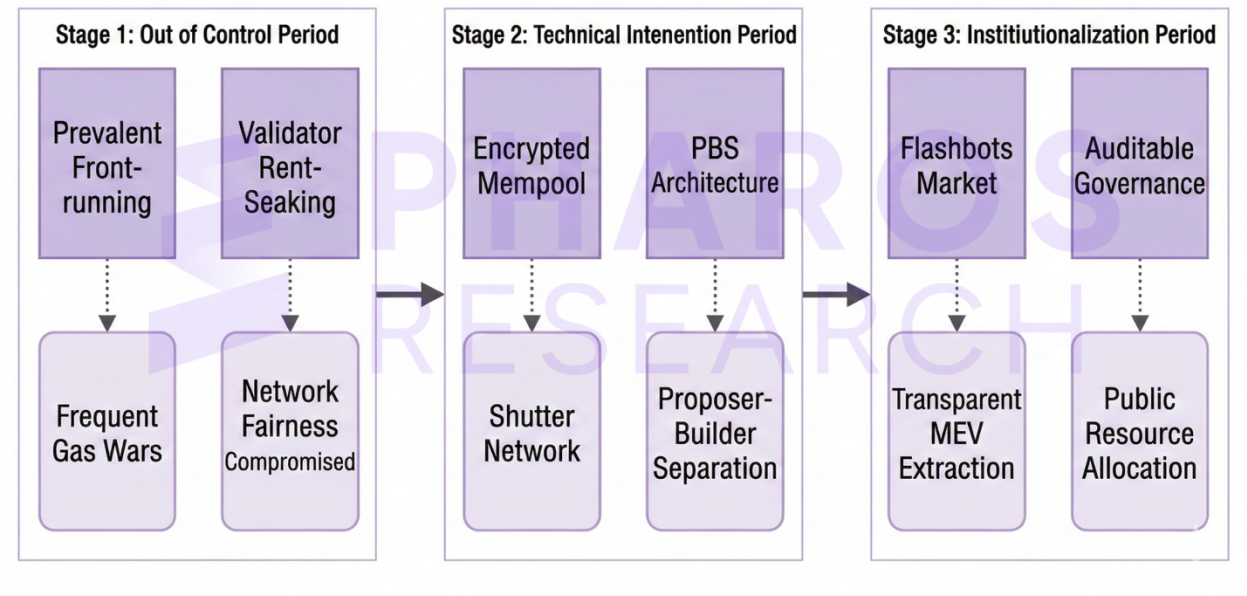
quantum-safe signatures without changing addresses, while ECDSA wallets based on BIP32 (such as existing accounts of Bitcoin and Ethereum) cannot realize backward-compatible smooth migration.[4] Ethereum Layer 2 ecosystem compresses the privacy and verifiability of transactions onto the chain through ZK-Rollups and ZK-STARKs, decoupling verification cost from data availability. This is not only a scaling method, but also a security preposition – moving complex computations off the main chain while ensuring that the results cannot be tampered with through mathematical proofs.

- The risk isolation value of modular architecture. The separation architecture of "execution layer – settlement layer – consensus layer – data availability layer" led by Celestia is becoming a security model for modular public blockchains. Its core contribution is that vulnerabilities in a single component no longer directly spread to the whole system. The evolution path of Ethereum Danksharding also follows this logic, reducing the impact of single-point failures on network finality by decoupling data availability from consensus. The Movement Labs hackathon report disclosed by Immunefi in 2025 pointed out[5] that if Celestia nodes incorrectly use blob.GetAll instead of blob.Get to retrieve data availability blobs, attackers can inject malicious blocks to cause full-node forks – the discovery of this vulnerability precisely confirms the importance of component boundary definition in modular architecture. The evolution path of Ethereum Danksharding also follows this logic, reducing the impact of single-point failures on network finality by decoupling data availability from consensus.

Economic and Game Strategy

- The dynamic equilibrium of staking and slashing. PoS public blockchains generally introduce slashing mechanisms to impose economic penalties on behaviors such as double-signing and long-term offline. However, the effectiveness of slashing depends on the dynamic matching between penalty intensity and network value: too light to form deterrence, too heavy will inhibit the willingness of small validators to participate. Ethereum embeds slashing conditions into the composite constraints of the beacon chain and sync committee, forming a reference model that balances security and decentralization.
- MEV from out-of-control to democratization. The vicious competition of MEV was once a major threat to the fairness of the Ethereum mainnet. The industry's response strategies have shifted from early passive laissez-faire to active guidance and power decentralization: Shutter Network and other encrypted memory pools prevent front-running; Proposer-Builder Separation (PBS) disassembles block construction rights and proposal rights through auction mechanisms to curb validator rent-seeking; Flashbots Auction establishes a transparent market for MEV extraction. These mechanisms jointly seek rebalancing between efficiency and fairness, turning MEV from a "dark forest" into an auditable and governable public resource. The three-stage evolution of MEV governance is shown in the figure below:

Figure 2: Three-Stage Evolution of MEV Governance



Source: Pharos Research

Ecological and Governance Strategy

- Roadmap and hybrid model of decentralized governance
  Almost no public blockchain achieves fully decentralized governance at the genesis stage. The key is to set a clear and predictable roadmap for decentralization. Ethereum was guided by the foundation in early research and development, and gradually transitioned to the EIP (Ethereum Improvement Proposal) process and full community consensus; Polkadot directly adopts an on-chain governance and treasury system, allowing token holders to vote on fiscal expenditure and protocol upgrades. In practice, the hybrid model of on-chain governance (efficient but vulnerable to vote-buying attacks) and off-chain social consensus (slow but Sybil attack-resistant) has become the standard configuration for mainstream public blockchains to avoid governance attacks.
- Developer incentives and audit transparency
  Top public blockchains generally set up special security funds and bug bounty programs. Immunefi platform has paid out more than $160 million in bounties[6], covering more than 900 projects, registering more than 90,000 white-hat hackers, with a maximum reward of $10 million for a single serious vulnerability, turning white-hat hackers into professional co-builders of the security ecosystem. At the same time, top DeFi protocols have formed an industry practice of cross-verification by multiple audit institutions, and complete audit reports are disclosed on the chain. More than 80% of the top 50 TVL protocols adopt cross-audit by at least two audit institutions, and complete audit reports are disclosed on the chain through Dune Analytics or GitHub, making security transparency a direct source of market competitiveness.

Operation and Response Strategy

- Diversity of clients and infrastructure
  The incident that nearly 80% of nodes on the Ethereum mainnet were abnormally synchronized due to the memory pool vulnerability of the Geth client in 2023 was a landmark case of client homogenization risk. Since then, mainstream public blockchains have begun to actively incentivize multi-client ecosystems – Ethereum supports alternative clients such as Nethermind and Besu, and Solana introduces Firedancer to reconstruct node software. At the same time, node deployment has also shifted from "single cloud vendor" to multi-cloud/hybrid cloud architecture to reduce the systemic impact of single-point failures of cloud service providers on network availability.
- Institutionalization of on-chain monitoring and emergency response
  Establishing real-time on-chain monitoring dashboards is becoming an industry standard. Key indicators include: block reorganization depth, validator staking concentration, abnormal cross-chain bridge traffic, precursors of stablecoin de-pegging, etc. The vigilance committee set up by Ethereum on the eve of the mainnet merger (composed of core developers, client teams and independent security experts) provides a reference paradigm for the industry's emergency coordination mechanism – when protocol-level risks break out, it can achieve limited and transparent temporary intervention without sacrificing the principle of decentralization. The number of global cross-chain bridge attacks decreased by 35% year-on-year in 2023[7], partly due to the popularization of real-time monitoring and response mechanisms.
- Infrastructure of user security education
  Security standards at the ecological level are changing from "optional" to default infrastructure at the application layer. The session verification specification of WalletConnect effectively reduces the success rate of phishing signatures; anti-SIM swap attack guidelines have been built into the interaction processes of many mainstream wallets; hardware wallet signature visualization makes transaction intentions clearly displayed on physical devices. These practices shift security awareness from user responsibility to platform responsibility, which is a necessary step for the public blockchain ecosystem to move towards mainstream adoption.

This framework clearly shows that public blockchain security is a dynamic strategy system running through consensus mechanisms, economic games, governance rules and operational disciplines. The value of differentiation lies not in judging which is superior or inferior, but in clarifying the coordinates of each public chain in the security spectrum; the significance of defense-in-depth is to reserve sufficient buffer and error correction space for unknown threats on the premise that "absolute security does not exist".

2.3 Comparison of Public Blockchain Security Risks

The security choices of different participants in the market essentially reflect the differences in their business positioning and value propositions.

Figure 3: Comparison Table of Mainstream Public Chain Architecture Types and Security Risk Control Features

Type	Institutional-Grade Public Chains	High-Flexibility Public Chains	Strategically Integrated Chains
Top Public Chains	Pharos / JPMorgan Onyx	Solana / BSC / Base	Ant Group Jovay / OKX Chain
Differences in Core Security Objectives	Zero-error financial bookkeeping and compliance platform	Continuous guarantee of uninterrupted high-performance network	Establish an international channel for compliant interoperability
Natural Disadvantages of Technical and Operational Risks	Complexity of self-developed/customized code	Uneven quality of smart contracts in ecological projects (risk dispersion but large scale)	Security of cross-chain and bridging protocol contracts (complex attack surface, affecting the whole body)
Maturity Benchmark and Main Advantages of Relative Security Infrastructure	Benchmark: IT risk control system of Global Systemically Important Banks (G-SIB)Advantages: bank-grade network isolation, hardware security module (HSM) key management, 7x24 monitoring and remote disaster recovery, strong ability to resist large-scale targeted attacks	Benchmark: large Internet cloud service providers (such as AWS)Advantages: strong elastic scaling capability, global node dispersion, rapid response of open-source communities, high ability to defend against large-scale traffic attacks and quickly fix vulnerabilities	Benchmark: global compliance and risk control platform of multinational enterprisesAdvantages: balance regulatory requirements between the East and the West on the basis of controllable technology, realize the sharing and isolation of ecological risks
Best Adaptation Scenarios	Cross-border payment, cross-border settlement, RWA, high-compliance and strong-credit financial assets such as treasury bonds	DeFi, NFT, high-frequency trading, personal market driven by Meme culture	Large-scale cross-chain asset interoperability, trade finance, multi-fiat stablecoin settlement network

Source: Pharos Research

Pharos' responsibility for security goes beyond on-chain code, covering the entire value chain from physical servers to private key storage and then to third-party partners. This heavy-asset model that continuously extends its own security boundary provides an operating environment with the highest certainty and the least variables. By building the most stringent and transparent security system in the industry, it guarantees high-net-worth assets and institutions with extreme security requirements. Choosing Pharos, in a sense, is choosing to turn its profound security infrastructure into a moat for its own business.

03 / Sustainability Verification: Security Economics Under Value Liquidation

Security is essentially a public service that requires continuous investment of resources (including R&D, auditing, monitoring and infrastructure) for maintenance and upgrading, rather than a one-time project. The long-term effectiveness of any security strategy must be based on a sustainable economic model. If a public blockchain cannot generate sufficient income through its own economic activities to cover these costs, then its security commitment is like a bad check and will inevitably fail in the long run. The market is conducting cruel value liquidation and differentiated verification through on-chain cash flow.

The sustainability of security strategy must ultimately be tested by the economic model. Through the most honest measure of on-chain cash flow, the current security paths of public blockchains have shown three completely different economic paradigms, and their sustainability capabilities have also diverged accordingly.

The path of ecological public chains represented by Base and Hyperliquid is centered on building a cash flow-driven growth flywheel. In this type of model, security investment is a direct operating cost, but its goal clearly serves core businesses that can generate immediate income, such as high-frequency transactions and on-chain applications. The continuous handling fee income generated by user activities provides a direct source of funds for security and development, thus forming a positive cycle: security and experience improvement attract more users and developers, which in turn generates more income, and income is fed back to higher-level security construction. Therefore, the key indicator to evaluate the health of such public blockchains lies in their protocol income and fee-to-market value ratio, and their commercial essence is a trading platform profitable by scale and traffic.

Public chains of the financial path represented by Pharos follow an access and trust-driven asset custody logic. Here, huge investment in security and compliance is the value of its core products. Its target customers are banks, asset management companies and RWA issuers, and these institutions prioritize the demand for security certainty far over transaction costs. Therefore, its economic model is similar to that of custodians or service providers in traditional finance, requiring extremely high capital expenditure in the early stage to build financial-grade infrastructure, and long-term income depends on the total scale of custodial assets and service fees, node license fees, etc. charged to institutional clients. The key verification indicators of its success are the total value of custodial assets and the quality of institutional clients, and security costs are regarded as a necessary entry fee to acquire and serve high-net-worth clients.

In sharp contrast are public chains trapped in the zombie chain dilemma. They lack a viable economic model, with sparse on-chain economic activities and a serious inversion of income and market value. Security investment is unsustainable due to lack of cash flow support, leading the network into a death spiral of “inactive → no income → more insecure → more inactive”, and eventually collapsing in the market’s value liquidation.

To sum up, security is not only a technical issue, but also an economic issue. It is a choice between becoming a platform profitable by traffic scale or a provider profitable by providing extreme trust services. The market ultimately only rewards models that can generate real and sustainable cash flow, and on-chain income has become the cruelest yardstick to test real utility and security sustainability.

Pharos' choice is a secure world where institutions can safely entrust hundreds of millions of assets and the machine economy can operate independently under strict protection. In the long construction of the value Internet, what Pharos represents is not the fastest chain, but the most trustworthy cornerstone.

References

[1] PANews. Mainland to the Left, Hong Kong to the Right: The “Tale of Two Cities” in the Public Chain Layout of Chinese Securities Firms – Part 2 [EB/OL]. (2025-12-12)[2026-02-26]. https://www.panewslab.com/zh/articles/c8c76715-289b-454d-9da9-29e58af6ccea

[2] PANews. The Cruel Liquidation of the Public Chain Market in 2025: Prosperous Casinos, False Ghost Towns and VC Harvest Games [EB/OL]. (2025-12-18)[2026-02-26]. https://www.panewslab.com/zh/articles/7a9f1125-701d-473c-b7f3-eace0cee8e28

[3] PANews. New Observations on 9 Public Chains: Is the King of Public Chains About to Change? Solana’s Ebb and BSC’s Strong Rise [EB/OL]. (2025-09-26)[2026-02-26]. https://www.panewslab.com/zh/articles/f00a6d40-65b9-4ae1-8b90-d745fe9113bd

[4] PANews. OKX’s Strongest Public Chain “Circle”: Disassembling the 2025 Actual Combat Report Cards of 7 Major Chains Including OP, Base, Unichain [EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/43643932-35bb-4449-b1fe-e63d911d6aabb

[5] PANews. Can AI Become a New Narrative for Old Public Chains? An Overview of 7 Combinations of Public Chains and AI [EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/rh070jrd

[6] PANews. Four Top Public Chain Representatives Gather to Talk About the Road of Public Chain Technological Innovation [EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/D77724764

[7] PANews. New Public Chains Frequently Crash: Where Is the Future of Public Chain Stability? [EB/OL]. [2026-02-26]. https://www.panewslab.com/zh/articles/D94993654

[8] Odaily. 8 Daily Active Users? The Truth Behind the Data in the Public Opinion War Between Solana and Starknet [EB/OL]. [2026-02-26]. http://www.odaily.news/zh-CN/post/5208784

Contributors

Authors: Huijie Tang (𝕏@web3sensen)

Reviewers: Colin Su, Grace Gui, NingNing, Owen Chen

Design: Alita Li

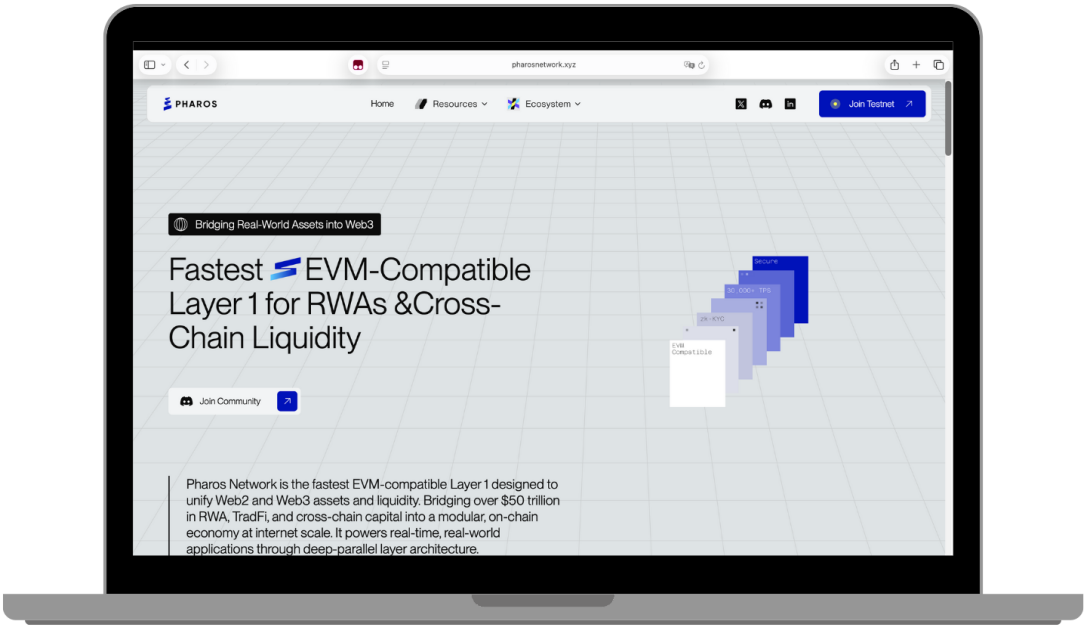
Disclaimer

This material is prepared by Pharos Research for the purpose of providing general information. It does not constitute and should not be deemed as investment, legal, accounting, or tax advice, nor does it form an offer, solicitation, or recommendation with respect to any securities, cryptographic assets, or strategies. The information and opinions contained herein may be derived from internal or third-party sources. While efforts are made to ensure their reliability, their accuracy, completeness, or timeliness is not guaranteed. Any decisions made and risks arising therefrom shall be borne solely by the reader. Past performance is not indicative of future results. This material may contain forward-looking statements (including forecasts and scenarios), which are subject to uncertainties and not guaranteed to be achieved. Cryptographic assets are highly volatile, and total loss may occur. They are also exposed to risks such as liquidity, technology, smart contract, counterparty, and compliance risks. To the extent permitted by law, the Research Institute and/or its affiliates or researchers may hold positions in the relevant assets, have business relationships with relevant entities, or otherwise have interests that may affect the objectivity of opinions. This material is not intended for persons in restricted jurisdictions. Reading, following, or subscribing to this material does not constitute a client relationship. Without prior written permission, no institution or individual may reproduce, copy, modify, or distribute this material. Any quotation shall be objective and complete, with the source clearly credited as "Pharos Research".

Contact

Pharos Network is a next-generation public blockchain for Real-World Assets (RWA) and stablecoins, focused on asset tokenization and on-chain circulation. We connect traditional institutions with the Web3 ecosystem, enrich the types of on-chain assets, expand revenue sources, and meet the allocation needs of a broader range of investors. Meanwhile, we help traditional enterprises unlock sustainable value on-chain through customized solutions. Boasting profound professional expertise and top-tier technical capabilities, our team builds a secure, efficient, and scalable infrastructure, providing institutions with a comprehensive decentralized ecosystem for onboarding assets onto the blockchain. We welcome strategic partners with a long-term perspective to co-build an open, compliant, and sustainable RWA ecosystem. For industry exchanges with us, please contact: chris@pharoslabs.xyz

Pharos' Official Website: https://www.pharosnetwork.xyz/



WeChat Official Account: Pharos Research

微信搜一搜

Pharos Research

PHAROS
RESEARCH

From RWA to On-Chain Finance.
Mapping Real-World Value.