LITEPAPER

Future-proof your digital assets with post-quantum security. Fast, scalable, and built to withstand tomorrow's threats

Date: 17/02/2025

Table of Contents

Abstract

As cyber threats rises and quantum computing advances, traditional cryptographic security methods are becoming increasingly vulnerable. By 2035, widely used digital signature algorithms (DSAs) such as RSA, EdDSA, and ECDSA will be rendered obsolete due to the capabilities of quantum computers. Recognizing this challenge, Armchain has been developed as a next-generation blockchain platform that integrates post-quantum cryptographic techniques to ensure security at the core level. Utilizing ML DSA 87 and a hybrid combination of Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) consensus mechanism, Armchain delivers a highly efficient and quantum-resistant blockchain solution tailored to meet the security demands of the future.

Introduction

The rapid growth of quantum computing presents a huge threat to current cryptographic standards, which underpin security across industries, including finance, healthcare, and national security. The National Institute of Standards and Technology (NIST), NATO Communications and Information Agency (NCIA), and the European Telecommunications Standards Institute (ETSI) have all emphasized the necessity for post-quantum cryptographic (PQC) solutions to safeguard sensitive data and digital transactions. With trillions of dollars in digital assets at risk, the need for a blockchain platform that is resistant to quantum threats has never been greater. Armchain aims to be that solution, offering a robust, scalable, and future-proof decentralized network.

The Need for Post-Quantum Security

Traditional cryptographic systems, including AES and RSA, rely on mathematical problems that can be efficiently solved by quantum computers using algorithms such as Shor's and Grover's. NIST's PQC initiative is focused on identifying and standardizing cryptographic techniques resistant to quantum attacks. Armchain is designed with these challenges in mind, integrating ML DSA 87, a state-of-the-art post-quantum digital signature algorithm that ensures robust security against quantum threats.

Beyond individual security, the implications of a quantum-resistant blockchain extend to industries reliant on secure digital transactions. Governments, enterprises, and financial institutions must prepare for a future where quantum computers can render existing security measures ineffective. The proactive implementation of PQC is no longer optional but a necessity.

"Vitalik Buterin proposes a hard fork strategy for Ethereum to protect funds against Quantum Computing attacks" – March 10, 2024

Armchain's Key Features

1. **Post-Quantum Cryptography**: Implements ML DSA 87 for quantum-resistant digital signatures.
2. **Scalability and Efficiency**: Utilizes a PoA/DPoS consensus mechanism to ensure high throughput, reduced latency, and lower energy consumption.
3. **Regulatory Compliance**: Aligns with NIST PQC, NATO NCIA, and ETSI standards to ensure cryptographic security.
4. **Advanced Security Model**: Offers an unparalleled level of protection beyond traditional AES/RSA-based cryptographic models.
5. **Smart Contract Integration**: Supports post-quantum secure smart contracts, enabling safe and future-proof decentralized applications (dApps).
6. **Interoperability**: Designed to seamlessly integrate with existing blockchain ecosystems, ensuring ease of adoption and migration.

Comparative Analysis

The table below compares top blockchain platforms based on their cryptographic mechanisms and vulnerability to quantum computing:

Blockchain	Signing Algorithm	Hashing Algorithm	Vulnerable to Quantum Threats?
Bitcoin	ECDSA	SHA-256	Yes
Ethereum	ECDSA	Keccak-256	Yes
Solana	EdDSA	SHA-512	Yes
Polkadot	EdDSA	Blake2b	Yes
Avalanche	EdDSA	SHA-256	Yes
Armchain	ML DSA 87	SHA3-512	**No**

Consensus Mechanism

Armchain utilizes a hybrid consensus model that combines Proof of Authority (PoA) and Delegated Proof of Stake (DPoS). This approach provides:

- **Scalability**: High transaction throughput with minimal computational overhead.
- **Security**: Resistance against Sybil attacks and Byzantine Fault Tolerance (BFT).
- **Decentralization**: Community-driven governance through delegated stakeholders.

This combination ensures both security and efficiency while maintaining a decentralized network governance structure that allows for adaptability in future upgrades.

Security Framework and Cryptographic Standards

Armchain follows the highest security standards outlined by NIST PQC, NATO NCIA, and ETSI, integrating:

- **Lattice-based cryptography**: Providing resistance to quantum attacks.
- **SHA3-512**: Ensuring integrity and immutability of blockchain data.
- **ML DSA 87**: A next-generation digital signature algorithm specifically designed to counter quantum threats.

Use Cases and Applications

Armchain's post-quantum security capabilities make it ideal for a variety of applications, including:

- **Financial Transactions**: Protecting assets in banking, DeFi, and digital payments.
- **Healthcare**: Safeguarding medical records and patient data.
- **Government**: Securing classified documents and communications.
- **IoT Security**: Preventing data breaches in smart devices.
- **Supply Chain**: Enhancing transparency and security in logistics networks.

Roadmap

Below is an overview of the planned milestones for Armchain's development:

Q2 2025: The Beginning of a New Era

- Tokenomics of ARMchain Coin
- Presale Live of Native Coin
- Early Access for Investors

Q3 2025:

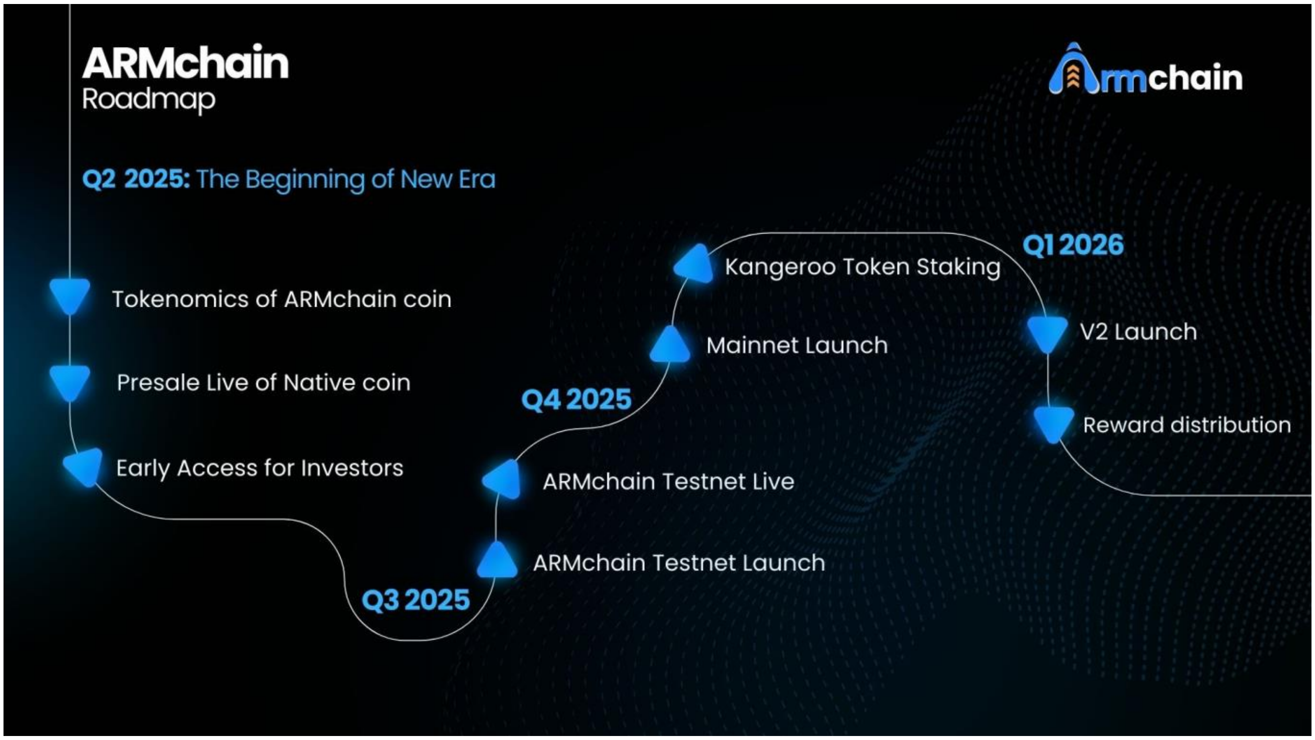
- ARMchain Testnet Launch
- ARMchain Testnet Live

Q4 2025:

- Mainnet Launch
- Kangaroo Token Staking

Q1 2026:

- V2 Launch
- Reward Distribution



ARMchain
Roadmap

Q2 2025: The Beginning of New Era

Tokenomics of ARMchain coin
Presale Live of Native coin
Early Access for Investors

Q3 2025

ARMchain Testnet Launch
ARMchain Testnet Live

Q4 2025

Mainnet Launch
Kangeroo Token Staking

Q1 2026

V2 Launch
Reward distribution

Conclusion

Quantum computing is evolving at an accelerated pace, posing a significant threat to existing cryptographic standards. Armchain provides a pioneering, post-quantum secure blockchain platform that ensures long-term security against emerging quantum threats. By leveraging ML DSA 87 and aligning with the world's leading cryptographic standards, Armchain is positioned as the most secure and future-proof blockchain available. Organizations and individuals looking for a scalable, efficient, and secure blockchain solution must recognize the necessity of adopting quantum-resistant technologies today to safeguard their digital assets for tomorrow.

References

- NIST Post-Quantum Cryptography Standardization: https://csrc.nist.gov/projects/post-quantum-cryptography
- NATO NCIA Cyber Security Initiatives: https://www.nato.int/cps/en/natolive/topics_82727.htm
- ETSI Quantum-Safe Cryptography: https://www.etsi.org/technologies/quantum-safe-cryptography