AlynCoin: A Quantum-Resistant Layer-1 Blockchain

Abstract

AlynCoin is a next-generation quantum-resistant Layer-1 blockchain designed to provide robust cryptographic security, full privacy, and scalability in a decentralized architecture. Featuring zk-STARKs, Falcon and Dilithium post-quantum signatures, and a unique hybrid PoW mechanism, AlynCoin is engineered for future-proof digital finance.

Vision

The vision of AlynCoin is to become the foundational layer of a post-quantum decentralized ecosystem. Our focus lies in enabling verifiable computation, on-chain privacy, and DAO-first governance while avoiding legacy architecture dependencies such as EVM.

Core Architecture

- Consensus: Hybrid Proof-of-Work using BLAKE3 and Keccak

- Cryptography: zk-STARKs for zero-knowledge proofs, Falcon and Dilithium for digital signatures

- Scalability: Recursive zk-Rollups for efficient L2 aggregation

- Storage: RocksDB Protobuf for fast, modular data handling

DAO Governance

AlynCoin is governed entirely on-chain through a 100 percent decentralized autonomous organization DAO. All proposals, votes, upgrades, and treasury decisions are executed via smart governance logic integrated into the core chain. There are no central authorities or multi-sig controllers.

Tokenomics

- Max Supply: 250000000 ALYN

- Initial Distribution: TBD

- Emission Schedule: TBD

- Use Cases: Transaction fees, staking future, DAO voting, L2 rollup collateral

Difficulty Adjustment

The difficulty adjustment algorithm is designed to maintain consistent block times. AlynCoin supports LWMA

AlynCoin: A Quantum-Resistant Layer-1 Blockchain

Linearly Weighted Moving Average and may evolve to an elastic difficulty system that adjusts based on network participation and transaction volume.

Roadmap Highlights

- Blockchain core with zk-STARKs, PoW, and post-quantum keys

- Wallets CLI plus GUI with L1 and L2 support

- Quantum-resistant NFTs and Atomic Swaps

- Recursive Rollup proof system

- Public Testnet and Mobile Wallet

- DAO Governance version 2 and zk-Escrow

- Mainnet Launch TBD

Contact

Website: https://www.alyncoin.com

Twitter: https://twitter.com/alyncoin

GitHub: https://github.com/ab1567/alyncoin-site

Email: contact@alyncoin.com