

Quantum-Resistant Cryptography for Blockchains

August 04, 2026 · Document #346 · bip39-phrase.com

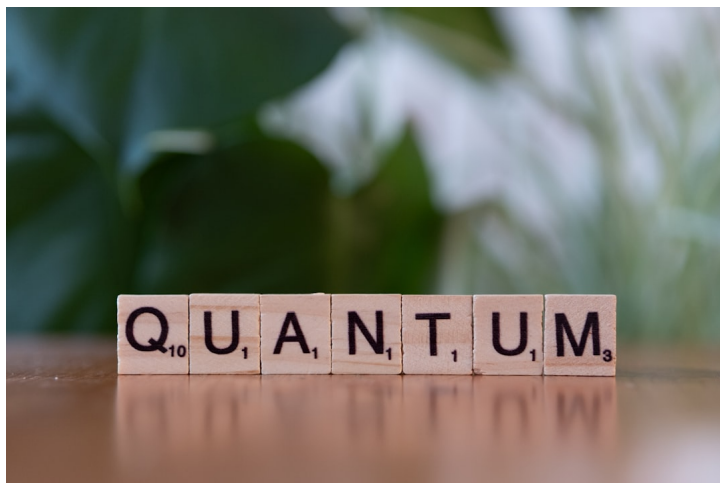


Photo by [Markus Winkler](#) on [Unsplash](#)

Most public blockchains rely on elliptic curve cryptography (ECC) to secure wallets and sign transactions. Bitcoin uses secp256k1; Ethereum uses a similar curve. A sufficiently powerful quantum computer running Shor's algorithm could derive a private key from a public key in polynomial time, breaking these schemes entirely. Current quantum hardware is nowhere near that threshold, but the cryptographic community treats the threat as a planning horizon, not a hypothetical.

Post-Quantum Algorithms and the NIST Standards

In 2024, NIST finalized its first set of post-quantum cryptographic standards: ML-KEM (formerly CRYSTALS-Kyber) for key encapsulation and ML-DSA (formerly CRYSTALS-Dilithium) along with SLH-DSA (based on SPHINCS+) for digital signatures. These algorithms rely on mathematical problems—module lattice problems and hash-based constructions—that have no known efficient quantum attack. For blockchains, the relevant concern is replacing ECDSA signatures used to authorize transactions and, in some chains, the hash functions underlying Merkle trees.

Integration Challenges for Existing Chains

Migrating a live blockchain to post-quantum signatures is technically and socially complex. Lattice-based signatures like ML-DSA produce keys and signatures that are significantly larger than their ECC equivalents: an ML-DSA signature is roughly 2.4 KB compared to 64 bytes for an ECDSA signature. This size increase affects block space, storage, and bandwidth. Chains with on-chain governance face coordination problems, since a hard fork is required to change the signature scheme. Ethereum's roadmap includes quantum resistance as a long-term concern, with EIP discussions around STARK-based account abstraction as one path forward. Bitcoin's more conservative development process has no finalized migration plan.

Another practical problem is the exposure of public keys. On Bitcoin, unspent transaction outputs that have revealed their public key—either through reuse or by spending—are theoretically vulnerable once quantum hardware matures. Addresses derived from hashed public keys retain some protection until the key is exposed during a spend. A migration strategy would need to move funds to quantum-safe address formats before the threat becomes real.

Chains Designed with Quantum Resistance from the Start

Some newer blockchains have incorporated post-quantum primitives in their initial design rather than retrofitting them. QRL (Quantum Resistant Ledger) launched in 2018 using XMSS, a hash-based signature scheme with formal security proofs. The Algorand team has published research on post-quantum secure state proofs. IOTA's earlier DAG-based design used Winternitz one-time signatures, though later versions moved to different cryptographic approaches.

The most defensible near-term position for blockchain developers is hybrid signatures—pairing a classical scheme like ECDSA with a post-quantum scheme so that breaking either alone is insufficient. This approach adds overhead but provides a transition period. As NIST standards mature and implementation libraries stabilize, the cost of adoption will fall. Chains that delay planning risk a disorderly migration once quantum hardware timelines become clearer.

Read more articles: bip39-phrase.com/p2p-crypto-trading/

WALLET RECOVERY WORDS

Below is a set of 64 randomly generated 12-word mnemonic sequences built from the official BIP39 wordlist.

- [] ring grit canyon easily match clever zebra mobile annual security addict purse
- [] canvas month indicate glue orchard frown hybrid trophy dawn tip daughter lecture
- [] unfold museum leisure rich cereal girl excess demise hobby fox bone girl
- [] steak film shed skin art knife analyst business cloth hobby stem bamboo
- [] mother weather owner borrow abstract chalk hen keep wheat ensure feed muffin
- [] toss short toss method opera vacuum loop squirrel drop funny three welcome
- [] flight gown crisp film tornado lamp target push concert garment box educate
- [] lamp laundry physical wine friend rain track fault happy stone oyster slam
- [] remove cushion advice stay target puzzle wealth behave already stomach pilot hello
- [] decade bone snack utility mystery lawsuit spend gym ranch shrimp blush vanish
- [] wasp elegant patch bid dirt vicious electric innocent duck grass rescue panic
- [] potato material leopard shed near there giraffe cupboard dune vague reward describe
- [] merit ribbon fee cabin people magic age picnic echo grab antique deputy
- [] pulp abuse local season comic perfect similar news science reduce action session
- [] item raccoon youth horror brisk acquire wealth citizen polar catch bread valve
- [] neglect bag deputy erupt negative rhythm innocent economy exchange reform vague limit
- [] dress rival cup kiss two float clog relief conduct dwarf impulse sense
- [] element machine adult surge input gain draft stereo polar cancel gun banana
- [] receive unfair palm base equip type face milk link wish breeze outer
- [] distance soccer citizen boss clown yellow dune better strategy catalog idle wool
- [] strategy license obey spy force memory acoustic gorilla captain rack gym river
- [] mesh frozen april auto grape toy advice hire busy toy approve truly
- [] scrap believe emotion cinnamon connect where ranch swallow crater arch popular survey
- [] churn sound thrive hover mask lend envelope call airport gas bind hire
- [] initial glimpse health cliff culture excess banana country any shoot domain message
- [] trick theme couch pear real walnut cheese salad proud topic impose crack
- [] oblige brother sauce elder habit thrive olive royal year pact produce staff
- [] level forest appear weapon arctic worry unhappy ranch lion world copper rate
- [] glide era wise nominee sand neither since cattle near puzzle review science
- [] hybrid between mimic permit soon jazz circle movie emerge between pitch supply
- [] possible convince park media crisp disorder slush clog argue clarify love onion
- [] obey tool elevator pet tomato face easy side wage change need position
- [] shallow defy host domain cloud cost fall sample leave dilemma pyramid mother
- [] ticket warm drill eagle material boy fan shrimp detect special honey celery
- [] gallery angry catalog notable rather menu advance extra market slender embody early
- [] donate require business ask employ illness refuse post jacket raccoon give unique
- [] dirt enrich dial celery abstract usual emerge oppose spare worry turn grow
- [] expect expect major false rival sure father science story link fashion affair
- [] supply prefer turn drum world onion version sport machine together minor easy
- [] attitude they room jaguar trust country rice poet spray trust ring reveal
- [] save stomach silk crowd song fresh gospel amateur vessel decrease expand subject
- [] right air else oyster surprise seat choice identify return finger oil assume

August 04, 2026 · Page 3

WALLET RECOVERY WORDS

[] drip rescue road tower layer walk tragic source recipe crucial doll maid
[] idle target click test page wagon rubber later clarify team emerge fashion
[] lunch rail slush announce walnut rabbit animal demand captain remember hobby put
[] cabin exile napkin item water prize donate vague general tongue vital nephew
[] expose hospital result execute aspect shallow useful disorder salute elite diagram fringe
[] ahead kiss raven secret slight avoid soccer minor flush virus globe quarter
[] initial alter promote token then picnic know ring sample inner play peace
[] invest obvious multiply mix vacuum evolve bargain arrest agree proof work ordinary
[] miracle unaware anxiety coconut above wrap leopard sun tent route maximum unveil
[] chat arrive turkey win zero nut matrix icon forum mesh arctic toward
[] accident wonder glide allow hurdle monkey circle envelope hollow churn kite another
[] trim cry obey nose rookie found ozone chalk test budget rocket tourist
[] jacket capital edit average soccer unusual melt payment below wild bone key
[] prevent around sustain enough mean actor sniff lawn park junior indoor base
[] welcome term group frost fit describe pattern sad steel exclude clever marriage
[] banana panic common unfold earn furnace leaf rally long ignore coffee toward
[] settle action secret time drama tower crater tone path culture ancient reunion
[] afford devote mention argue retire logic lab tray egg catalog limit witness
[] picnic cabin master control where join fuel winner hood slender still typical
[] ready kingdom open humble pattern sun hand strong vacuum cruise planet coffee
[] turn impulse first height razor bamboo release tooth hunt drama melt path
[] object dream raccoon summer hill comfort submit banner rocket deny actress infant

SEE ALSO

- [Understanding Cryptocurrency Wallets: Your Digital Asset Guardian — BIP39 Seed Phrases](#) (March 30, 2026) (2026-03-30)
- [How Whale Movements Affect Crypto Prices — BIP39 Seed Phrases](#) (June 24, 2026) (2026-06-24)
- [The Rise of Play-to-Earn Crypto Games: Revolutionizing Digital Entertainment — BIP39 Seed Phrases](#) (April 13, 2026) (2026-04-13)
- [what-is-infura-bip39-phrase_2025-11-12.pdf \(bip39-phrase_2025-11\)](#)

Educational examples only. Randomly generated, not valid wallet phrases - never use them to store funds. Details: bip39-phrase.com/security/

August 04, 2026 · Page 4