

Quantum-Resistant Cryptography for Blockchains

August 13, 2026 · Document #355 · bip39-phrase.com

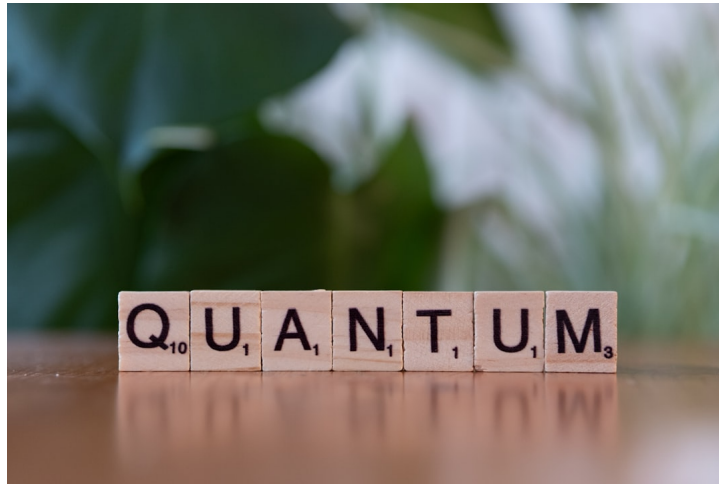


Photo by [Markus Winkler](#) on [Unsplash](#)

Most public blockchains rely on elliptic curve cryptography (ECC) — specifically ECDSA — to secure wallet addresses and sign transactions. A sufficiently powerful quantum computer running Shor's algorithm could derive a private key from its corresponding public key in polynomial time, breaking the security assumption that underlies Bitcoin, Ethereum, and most other chains. Current estimates put the threshold at roughly 4,000 logical qubits for a viable attack, a capability that does not yet exist but is considered a credible long-term risk.

Post-Quantum Algorithms Under Consideration

In 2024, NIST finalized its first set of post-quantum cryptographic standards. ML-KEM (formerly KYBER) addresses key encapsulation, while ML-DSA (formerly DILITHIUM) and SLH-DSA (formerly SPHINCS+) handle digital signatures. These algorithms derive their security from problems believed to be hard for both classical and quantum computers — primarily lattice problems and hash-based constructions. For blockchains, the signature schemes are the most relevant, since transactions require compact, verifiable proofs of authorization.

The practical challenge is overhead. A standard ECDSA signature is 64 bytes. An ML-DSA-65 signature is approximately 3,293 bytes — about 51 times larger. SLH-DSA signatures range from 8 KB to 50 KB depending on the parameter set. At current transaction volumes, adopting these schemes without protocol changes would dramatically increase block sizes, raise fees, and strain node storage.

Migration Challenges for Existing Chains

Migrating an active blockchain to post-quantum signatures is not a simple upgrade. Addresses derived from public keys — as Bitcoin's P2PKH addresses are — expose the public key only at spend time. Funds sitting in unspent outputs with unexposed public keys retain some protection, but any address that has already sent a transaction has a visible public key and is vulnerable once quantum attacks become feasible.

Ethereum's account model exposes public keys immediately upon first transaction, making its existing address space more uniformly vulnerable. Both ecosystems would require hard forks, a coordinated transition period, and likely a cutoff block after which old signature schemes become invalid. Users who lose access to keys before migrating would lose funds permanently, since there is no central authority to recover them.

Current Development Efforts

Several projects are already building quantum-resistant chains from scratch or adding hybrid signature support. The QRL (Quantum Resistant Ledger) launched in 2018 using XMSS, a hash-based signature scheme. Ethereum's roadmap includes research into post-quantum account abstraction as a migration path, allowing wallets to upgrade their verification logic. The Ethereum Foundation has discussed a hard fork that would allow smart contract wallets to implement ML-DSA natively.

Bitcoin's path is more constrained by its conservative governance model, though proposals such as a new SegWit-style output type for post-quantum keys have been discussed informally. The consensus among researchers is that the transition needs to begin before quantum threats are imminent, because retroactive migration at scale — moving trillions of dollars in assets safely — is an unsolved coordination problem.

BIP39 RECOVERY PHRASE LIST

Below is a set of 56 randomly generated 12-word mnemonic sequences built from the official BIP39 wordlist.

1. cube guide tree upgrade popular twist panic library glare enjoy private phone
2. alert attack tuition acid galaxy cake march amount regret grow debate essence
3. few drive spawn modify romance panic rug hollow talent occur candy jungle
4. chapter math always area fringe before flight umbrella absorb divert eyebrow tiger
5. antenna acid that effort glance ticket doctor input analyst trophy jar update
6. arrange grunt eight such label bid black deal immune move box turtle
7. crew father aisle gospel crack blood original purse shallow bargain melody despair
8. lamp reflect true social panther invite loan memory emerge circle execute boost
9. envelope dismiss library manage improve arctic spoil artwork asset reopen any history
10. bench belt plastic table jealous battle system success ordinary deposit palm argue
11. region private matrix metal swim minute example cereal can inner enable lady
12. win shadow tower warfare enrich drink discover enable reopen charge barely lava
13. venue dice wide praise shy dismiss puzzle such coin minimum wheel sword
14. stand stick audit inhale balcony seven write recall solve parade current under
15. milk domain orchard route tired silly movie hat post autumn captain impose
16. immense crush novel digital survey goddess panel champion tool small sunny useful
17. fury upon remain effort inquiry mass endless melt same cannon adult despair
18. damp response grocery drastic swim before alarm annual render flip another more
19. obtain frown candy hello stumble expect setup increase memory warfare hole seminar
20. put castle plate knock wedding movie warrior measure spike install auto robot
21. choose ability honey report render minute blind soup shield brass cube hand
22. region carbon stuff demand surprise desert move payment grid cable gospel network
23. holiday between loop strong dynamic exhibit airport citizen dentist concert various have
24. trouble series spin term harbor virus fat rocket chicken orchard add high
25. judge bubble oil hurt depart garlic glimpse actual convince various hybrid route
26. peasant leave outside detect describe hole faint source road critic inherit armed
27. electric success effort blossom humble cross friend hold stereo gas smoke wine
28. romance private empty wear sight illegal item student hamster mansion coin quit
29. radio visa blade devote citizen child zero focus network hybrid double table
30. shuffle fantasy slush wheel provide gain burger digital clog lizard still reopen
31. final wisdom hand goddess present rigid library void chair goose motor process
32. marble violin blossom common naive void spirit exotic shadow casual hover spread
33. estate equal light solve arch oblige slow seed gather tissue hill bean
34. album nice cheese autumn very reopen venture credit blouse rent setup relax
35. midnight very rocket project doll raven deputy way kiss defense couple slight
36. tobacco nice glad flat upon dragon sure morning vivid praise online better
37. random foster original tell immense furnace hollow catalog anxiety adult order party
38. boss liar tissue task wink dwarf outdoor destroy forest genius edit detect
39. cause frog glory parrot clip census uphold despair thrive chicken fire mouse

bip39-phrase.com · 3/4

BIP39 RECOVERY PHRASE LIST

- 40. visa clip poverty east crunch exit parrot library banner trust home annual
- 41. ball motion hurt ethics autumn tank dish gold private funny leader mask
- 42. corn rose force zone fragile gold heavy park solid update extend math
- 43. avoid dragon draft swamp stadium ocean scene diesel grain spare upgrade since
- 44. crumble stumble dizzy dose critic relief creek ship cactus dash topple kid
- 45. vibrant slide swift truck better obscure pass teach frame note explain deal
- 46. flee ketchup trumpet start decrease cat garden hidden modify wide powder culture
- 47. option enforce alarm ritual kangaroo ecology ensure legend base develop suit industry
- 48. guard social turn brick swap stereo aware shoot snack first century wrap
- 49. keep trouble stuff nominee fame marble rhythm frequent salt protect economy rifle
- 50. secret wheel smart spirit demand input machine winter acquire chalk travel firm
- 51. merry sure stock disagree flee minute spread potato major rapid bench deposit
- 52. choose fortune swing measure task cereal idle outdoor gasp release organ jealous
- 53. family shy mesh host index safe vital blind air marine plug sunny
- 54. erode riot divide opera fabric top discover alcohol course notice creek shy
- 55. advance deliver symbol course front expand input jungle roof stadium old clog
- 56. follow vacuum also heart uncle trouble obtain cook abuse advance again garage

SEE ALSO

- [Quantum-Resistant Cryptography for Blockchains — BIP39 Seed Phrases \(August 04, 2026\) \(2026-08-04\)](#)
- [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 \(April 13, 2026\) \(2026-04-13\)](#)

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

bip39-phrases.com/security/

bip39-phrases.com · 4/4