

Quantum-Resistant Cryptography for Blockchains

September 25, 2026 · Document #396 · bip39-phrase.com

The Threat Model

Blockchains secure ownership with public-key signatures: ECDSA over secp256k1 in Bitcoin, Ed25519 in Solana and Cardano, BLS12-381 for Ethereum consensus. All of them rest on the hardness of the elliptic-curve discrete logarithm problem. Shor's algorithm solves that problem in polynomial time on a fault-tolerant quantum computer. Published resource estimates for breaking a 256-bit curve range from a few thousand to a few million physical qubits, depending on error-correction assumptions, so no credible attack timeline exists. The risk is archival. Every block is permanent, so a public key exposed in a 2015 transaction stays attackable forever. Coins on reused addresses, and every chain with a transparent ledger, face retroactive exposure.

What NIST Standardized

NIST released its first post-quantum standards in August 2024: FIPS 203 (ML-KEM, from CRYSTALS-Kyber), FIPS 204 (ML-DSA, from CRYSTALS-Dilithium) and FIPS 205 (SLH-DSA, from SPHINCS+). ML-DSA is the closest fit for transaction signing. SLH-DSA is slower and larger but depends only on hash-function security. Symmetric primitives need far less change: Grover's algorithm gives a quadratic speedup against preimage search, cutting SHA-256 from 256-bit to roughly 128-bit security, which remains acceptable. Falcon, selected alongside Dilithium in 2022, is being standardized as FN-DSA; as of early 2025 that draft was not final. Falcon-512 produces signatures of about 666 bytes and public keys of 897 bytes, while ML-DSA-44 signatures are 2,420 bytes. That size gap drives most engineering decisions.

Costs of Migration

A Bitcoin ECDSA signature occupies roughly 71 bytes. An ML-DSA-44 signature is about 34 times larger, and an SLH-DSA signature roughly 110 times larger. Because block space is priced by weight, a naive swap multiplies the cost of every transaction and shrinks throughput. Mitigations exist. Falcon and its FN-DSA successor keep signatures near 666 bytes. Signature aggregation, using STARKs or recursive proofs to compress many post-quantum signatures into one, is an active research direction on Ethereum. The Quantum Resistant Ledger has used the stateful XMSS hash-based scheme since 2018, which avoids lattice assumptions but requires careful one-time key management and caps the number of signatures per key.

Wallet and address formats are the harder problem. Most addresses are hashes of public keys, which hides the key until spending; that is a weak but real protection. Migrating means changing key derivation, transaction serialization, hardware-wallet firmware and every indexer at once. Hybrid schemes requiring both an ECDSA and a post-quantum signature during the transition are the conservative choice, and crypto-agility, meaning signature verification that can be swapped without breaking consensus, is now a stated goal for several protocols.

Timeline and Priorities

No one is spending quantum-vulnerable coins today. The practical work is inventory: locate keys with long exposure windows, standardize hybrid verification, and keep signature algorithms behind an upgradeable interface. For chain developers, the sensible assumption is that whatever scheme is chosen now should be replaceable within a decade, without a hard fork of historical state.

Read more articles: bip39-phrase.com/blog/

Contents: Article (p.1) -> Seed Phrases (pp.2-4) -> Related Documents (p.5)

BIP39 MNEMONIC COLLECTION

Below is a set of 96 randomly generated 12-word mnemonic sequences built from the official BIP39 wordlist.

[] cattle faint shy letter only flag clip remember issue space stamp bicycle
[] despair bronze side tribe immune author aim piece stone yellow stumble setup
bip39-phrase.com · 2/5

BIP39 MNEMONIC COLLECTION

- [] jacket captain impose danger cruise uniform grit ladder rubber day gossip glow
- [] analyst august connect safe faith print cause old economy tooth trash elephant
- [] across april worth total orange bird limb shuffle noodle jungle pond name
- [] grass attack leg own kick agree best panel album print magic spike
- [] birth slot absorb embrace energy across gain ozone two example under session
- [] give cricket cabin various brain dish tuna plastic hand home pulp ostrich
- [] game practice decide host huge grit crawl return inside nothing number you
- [] view anger hungry cram relax rabbit depend clean execute add hole change
- [] logic clarify moment tongue hint utility fire sad mother despair armor dolphin
- [] yard barrel program victory glad find transfer solution credit ten ticket betray
- [] easy tumble story lady aerobic slab spirit weather spray exercise stairs expand
- [] axis alley ocean age search mail hunt shed prefer retire major sniff
- [] couch master practice observe wide you must own share bind noise chair
- [] stand cube hint nose sell join gold online lunch era truth youth
- [] pudding purity unveil easy rubber finger sword route clog rifle shoulder margin
- [] angry few below chicken family tobacco culture giggle island cake duck choice
- [] robot team state whisper concert sudden kid proud link approve club helmet
- [] put bind train axis utility luxury abstract foster vault vicious belt radio
- [] social fox nominee junk mimic club tuna private neutral gold buffalo gaze
- [] banner reform drill parrot diesel move depend jump pencil river tree assist
- [] luxury bounce special fossil range chapter duck club world shine provide captain
- [] antenna jaguar all upper waste surprise emotion skull tongue friend tattoo dial
- [] will ocean capable reflect corn civil chalk now sorry cabin kick decade
- [] short entry become buzz suffer waste basket taste change culture zebra ghost
- [] dismiss blame suspect butter spring orbit garage shallow galaxy girl segment copy
- [] blossom resist bounce yard knife obey moment umbrella attend screen guess key
- [] betray reform benefit card city ten dawn weapon swarm mistake include visit
- [] voice grant toast relief measure bring awesome element candy ripple frog scheme
- [] bubble pepper entry fiber spray mind clog ball leaf focus basic rhythm
- [] number route note miracle goose negative shield farm bridge unhappy thought member
- [] amused gossip wire muscle coast purity next hat expire riot enhance panic
- [] crash area category evidence debris build armed moral wreck start pilot volcano
- [] drip wasp liquid soap giggle alter pyramid cancel report ripple shiver drive
- [] question chaos embark hungry expose price duty spray warm shine claim rocket
- [] flag common joke test whisper twin gospel mosquito general fitness throw jealous
- [] endless bunker scene average people shoulder distance decorate photo wing nose raise
- [] alien deputy ignore river injury amazing okay practice summer deer popular decade
- [] punch ripple crouch answer flash tourist chef theme bubble intact enroll dream
- [] polar solar math shed fever leaf wait harbor orphan price sorry object
- [] brown stumble cabbage thunder diagram organ busy venue success enable bicycle try
- [] zero hole gown expect sense under soldier venue source seat other anger
- [] blue engine latin love leisure differ grow valley win arrange wrong accident
- [] sand celery orange humor submit fiction march deny damp cinnamon auction sibling
- [] fat submit smile better credit process mule canyon carpet orient peasant blue

bip39-phrase.com · 3/5

BIP39 MNEMONIC COLLECTION

[] capable manual peanut risk confirm fiction off visa truck confirm skill mirror
[] yellow legal flip leisure soup door wish input lift cabin story parade
[] pledge short select emotion debate humble weasel dirt blue method certain gain
[] diesel clog range drop suggest kind ordinary entire wet crisp crop trip
[] piece grunt combine able photo siege pulp define patient purpose uncover axis
[] convince rather wagon rebuild town bonus patient logic fence town sauce resource
[] social unfold fade govern seven copy angry eager just sure actual foster
[] hollow humble scene crazy engage obtain sting work only frog defy torch
[] dwarf unable panda they glare attend spray arena two better swarm nothing
[] evoke egg doll inch when daring fetch thunder luggage silly defense shell
[] shed vague chunk slight caught endless ten enough deny addict foam body
[] hub armor miss all false maze accident caught worth tiny leg about
[] warfare gesture memory mechanic input festival sniff aware brass brave mutual submit
[] horror mass artist merry mobile wage wedding negative dentist message balcony ghost
[] collect casual arena follow champion caught case venture have present purchase wagon
[] drama ritual column buffalo shine view minute insane then diagram tent hard
[] evolve vendor bundle nose search spirit benefit knee stuff method notice prepare
[] neither thought like entry return worth rude ensure wrap winter there rebuild
[] hunt car hidden salute ribbon stomach quantum clay fox fabric science achieve
[] prepare cover rifle wage ordinary message media rose flavor kitten liquid museum
[] tattoo faint myself hunt leave price kiwi silent essence grab leader holiday
[] tide spot ripple envelope waste arrest fine shuffle dizzy bag scissors force
[] dream garlic that genre brass render recycle around exist cereal extra usage
[] scare wet harsh else boss auto wedding safe faint angle truck quality
[] silent impact tape opera amazing still wine eye wheat range candy walnut
[] toy much outside defy bracket increase knock era cave pony bitter devote
[] train pattern vessel kangaroo pitch erupt expose blur robot debris donor high
[] provide team throw example danger cash solar process fame insane just liberty
[] style output torch crater wine myth evil hundred okay gloom exist combine
[] fatal transfer twice explain outside deer universe motion size cat employ sugar
[] sustain narrow limb club plate super myself surprise spring purity creek spend
[] buffalo cave hockey onion unhappy file profit divorce smart uncle emerge satoshi
[] wine tragic sun orphan vapor surface oil extra explain primary abuse top
[] just civil shop behind caution gentle fork year grain bomb strike move
[] prefer color luxury steak hungry hurdle castle glow memory shield bracket wave
[] record long fault child south drink tide argue lottery code ridge affair
[] option ranch foil silent school sun sure dizzy neck minor merge spray
[] book pistol moment liquid hollow sense cloth engine immune unit pupil father
[] guitar spirit soon urban elite rather salad anxiety bargain bulk river believe
[] episode federal engine crystal enact between lift enter plug tunnel eager dice
[] flip shoulder fury injury nominee athlete permit grow body echo acoustic appear
[] cube potato crunch rare thank medal live thunder salad mention broccoli liar
[] want arrive erode side vacuum category area surge frequent green blue matter
[] able trade stumble absent brother boss goddess fury monitor appear volume sheriff

bip39-phrase.com · 4/5

BIP39 MNEMONIC COLLECTION

[] sea shadow ozone hard long obey rocket scrap reject mouse grocery satisfy
[] orbit sadness river remember chef still cover bounce ladder swing ridge afford
[] fiber subway shift spatial bunker giraffe swear save brown decorate text muscle
[] decorate drastic small achieve common home spy gain include busy clock magic
[] cushion exchange hybrid cruel salt rib affair bleak join short figure scorpion
[] march hazard defy flag tooth left artefact pact wash clutch margin inherit

SEE ALSO

- [Proof of Work vs Proof of Stake: A Comprehensive Comparison — BIP39 Seed Phrases](#) (April 08, 2026) (2026-04-08)
- [How Decentralized Exchanges \(DEXs\) Work — BIP39 Seed Phrases](#) (March 31, 2026) (2026-03-31)
- [Introduction to On-Chain Analytics — BIP39 Seed Phrases](#) (June 09, 2026) (2026-06-09)
- [MEV: Maximal Extractable Value Explained — BIP39 Seed Phrases](#) (June 11, 2026) (2026-06-11)

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

bip39-pharse.com/security/

bip39-pharse.com · 5/5