QNN RESEARCH #04 • QUANTUM THREAT • 22 OCTOBER 2026

Noah’s Ark

a bunker for institutions

If a quantum computer broke Bitcoin tomorrow, where would you run? Five candidates, deep dives on QRL and Quantus (QTC), price forecasts.

Not financial advice • data as of 22 Oct 2026 • background: Ivan Aivazovsky, “The Deluge”, 1864 (public domain)

BEFORE WE START • DISCLAIMER

A bet on belief, not on a product

QRL and Quantus (QTC) **have no revenue-generating product**: no fees accruing to holders, no business and no financial reporting. Their value rests on a single expectation: that on the day of a quantum break they become **a "Noah's Ark" for crypto capital**, the place where large holders and institutions move their money once Bitcoin and Ether are under threat.

What holds the price up

Demand for insurance against quantum risk, headlines about quantum computers, and the expectation that institutions arrive via Strongpoint and major exchanges.

What is missing

Revenue, cash flow and profit. So a "fair price" cannot be computed with the usual tools, such as multiples or discounted cash flow.

What it means for investors

This is not a stake in a business but **an option on an event**: Q-Day. If Bitcoin upgrades in time, the ark may never be needed, and the price loses its main support.

Not financial advice. Only put into such assets an amount you are fully prepared to lose.

ONE-MINUTE SUMMARY

A refuge exists, but its door is narrow

Real threat, not tomorrow

Google (31 Mar 2026): breaking a Bitcoin key needs ~1,200 logical qubits. The best machines today have 48–96.

~6.9M BTC exposed

About a third of all bitcoin sits on addresses whose public key is already visible (Project Eleven, May 2026).

Refuge #1: QRL

8 years of post-quantum protection on every address, plus external audits. Downside: only ~$95K of daily volume.

Quantus (QTC): strong tech, no history

NIST-standard crypto from block one and the most audits. But the chain is 6 weeks old and 1.4% of coins circulate.

The trap is liquidity

All default-PQ coins together trade under $10M a day. In a panic the exit door is tiny.

Forecast to end-2027 (hypothesis)

QRL: base $1.5–3.5 (45%). QTC: base $40–110 (35%), but the bear case is likelier at 50%.

Sources: Google Research • Project Eleven • CoinGecko QRL • CoinGecko QTC

EXPLAINED SIMPLY

How a quantum computer steals bitcoin

1
Lock and key

Bitcoin is protected by a key pair. A secret key easily gives a public key; going back would take an ordinary computer billions of years.

2
The public key shows

When you spend, reuse an address or hold coins on an old P2PK address, your public key is visible on-chain.

3
The quantum locksmith

Shor’s algorithm on a large quantum computer runs it backwards: public key → secret key. Google estimates about 9 minutes.

4
The theft

The thief signs a transfer of your coins to himself. If your payment is still in the mempool, he outbids it: ~41% chance to win.

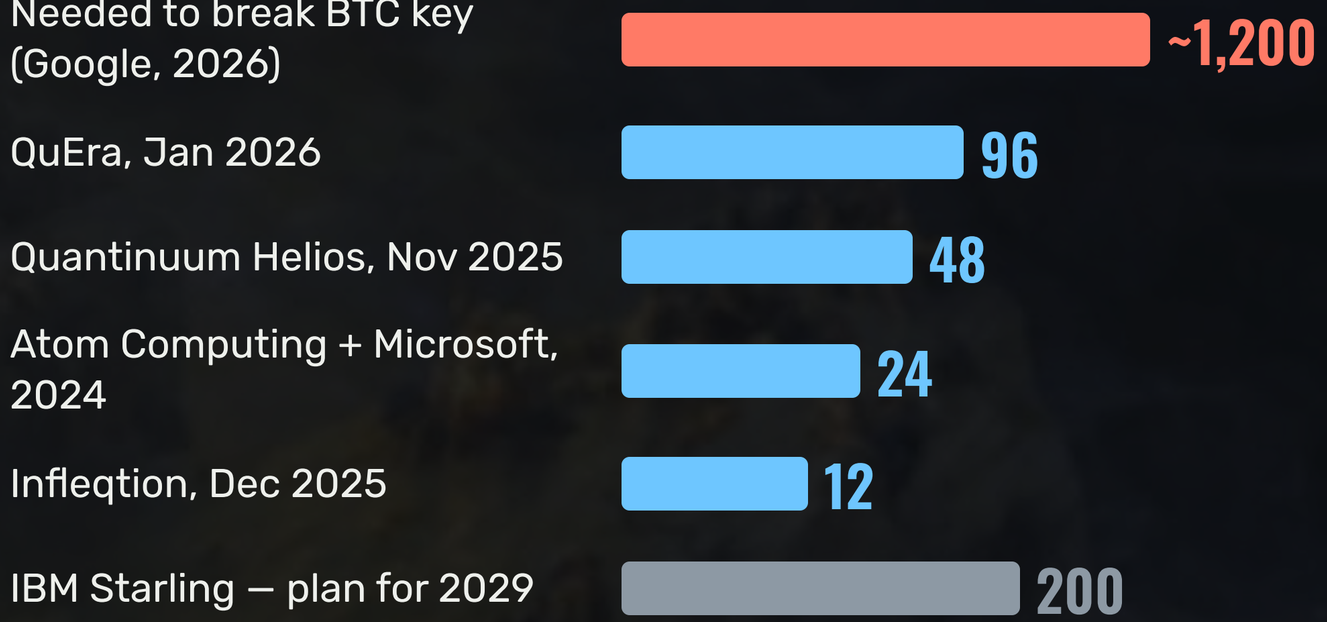
What survives: hash functions (a quantum computer only gives a square-root speedup against them). Signatures such as XMSS and SPHINCS+ are built on them; lattices (ML-DSA) are the other family. That is “post-quantum” protection. NIST standards ↗

Sources: Google blog 31.03.2026 • The Quantum Insider • NIST FIPS 203/204/205

THREAT • HOW CLOSE

The gap is still big: 96 of the ~1,200 qubits needed

Logical (error-corrected) qubits, log scale



<500,000
physical qubits suffice in Google's new estimate, 20× fewer than before

~9 min
per key on a "primed" machine; ~41% chance to snipe a mempool payment

6,100
atoms: the largest qubit array (Caltech, 2025), not yet a computer

Sources: Google • Logical qubit leaderboard • IBM • Caltech/TQI • Roadmaps

THREAT • WHAT IS EXPOSED

6.9M BTC already show their key



4.99 M
Reused addresses • 72.3%

1.72 M
Old P2PK (Satoshi era) • 24.8%

0.198 M
Taproot • 2.9%

~$560B
value of exposed BTC in May 2026 (The Block): ~33% of all supply.

~5.6M BTC
have not moved in 10+ years (Lopp). Owners may have lost keys and cannot migrate.

>65% of ETH
sits on exposed addresses (Deloitte, cited by Project Eleven). Ether is no safer.

Sources: Project Eleven report • PostQuantum • The Block • CoinDesk (Lopp)

THREAT • WHEN

Q-Day: 2028 to 2042, but deadlines are already set

When a dangerous machine arrives: forecasts

2028	Vitalik Buterin: a break is possible before the 2028 US election
2030	Project Eleven: optimistic Q-Day • Justin Drake: 10% odds
2032	Justin Drake: 50% odds
2033	Project Eleven: base case (“more likely than not”)
2042	Project Eleven: pessimistic case
2045+	Adam Back: “probably not for 20–40 years, if then”

When ECC must be dropped: deadlines

2027	NSA (CNSA 2.0): software and firmware signing must be post-quantum
2029	Google moves its own infrastructure to PQ; Ethereum Foundation target
2030	NIST: RSA-2048 and ECC P-256 deprecated; EU: critical infrastructure
2031	UK (NCSC): priority migration
2035	NIST: all vulnerable public-key crypto disallowed; NSA and NCSC complete

Sources: Project Eleven/PRN • Drake/CryptoTimes • Vitalik/CT • NIST/NSA/EU deadlines • NCSC • Adam Back

THREAT • WHAT THEY SAY

Voices: calm bitcoiners vs worried scientists

Michael Saylor
MicroStrategy/Strategy • 13.10.2026

“it’s probably a 90-day upgrade.”

source ↗

Michael Saylor
X • 16.12.2025

“Quantum computing won’t break Bitcoin — it will harden it.”

source ↗

Adam Back
Blockstream • 15.11.2025

“probably not for 20–40 years, if then.”

source ↗

Jameson Lopp
BIP-361 • 15.04.2026

“It’s not that I want to freeze anyone’s bitcoin.”

source ↗

Vitalik Buterin
Ethereum • Nov 2025

“elliptic curves are going to die”

source ↗

Justin Drake
Google paper co-author • 02.06.2026

Q-Day odds: 10% by 2030, 50% by 2032

source ↗

Charles Edwards
Capriole • Dec 2025

“If we haven’t deployed a fix by 2028… sub $50K”

source ↗

Scott Aaronson
quantum scientist • Nov 2025

Shor before the next US election is “a live possibility”

source ↗

BlackRock has listed quantum computing as a risk factor in the IBIT bitcoin ETF prospectus since 9 May 2025. filing ↗

THREAT • CAN BITCOIN DEFEND ITSELF

The cure exists, but only in drafts

BIP-360 • P2MR

A new address type without Taproot's exposed key path. Merged as a draft in Feb 2026, **not activated**. It does not replace ECDSA by itself; a separate PQ signature is needed.

BIP-361 • the freeze

Lopp's plan: after ~3 years ban sends to vulnerable addresses, after ~5 years freeze all legacy signatures. Draft, controversial.

Rescue via ZK

Prove you know the seed without revealing the key: Roasbeef prototype (Apr 2026, ~55 s per proof) and Project Eleven (Jul 2026).

Ethereum

In Jan 2026 the Ethereum Foundation formed a post-quantum team, targeting full migration by 2029. Vitalik described an "emergency hard fork" back in 2024.

Reality vs Saylor's "90 days"

Past Bitcoin soft forks took years: SegWit was proposed in 2015 and activated in 2017; Taproot 2018 → 2021. Then millions of users must move their own coins to new addresses, and lost keys never migrate. **[OUR VIEW]**

Sources: BIP-360 • BIP-361 • Roasbeef • Project Eleven • EF PQ team • Vitalik 2024

THREAT • SCENARIOS

Three quantum-strike scenarios [HYPOTHESIS]

A. Planned migration

Bitcoin and Ether migrate to PQ signatures by the early 2030s. Post-quantum coins stay a “theme”: they rise on news and fade in silence.

B. Slow leak

Old Satoshi-era P2PK addresses quietly start emptying. The market reads the signal, BTC drops hard, a rushed soft fork starts and money flees to PQ coins.

C. Sudden Q-Day

A secret machine at a state or corporation. Mempool thefts, exchanges halt withdrawals, bridges (themselves on ECC) freeze. PQ coins spike but there is almost nowhere to buy them.

~75%
scenario A through 2030, our estimate

~20%
scenario B

~5%
scenario C

Probabilities are our hypothesis, based on the qubit gap (96 of ~1,200) and Drake’s “10% by 2030”. Note: in scenario C, exchanges running ECDSA wallets become targets themselves.

Sources: Drake • Project Eleven • Google

THREAT • WHO IS PREPARING

Institutions are already building bunkers

Project Eleven

A startup measuring crypto's quantum risk. Raised ~$26M: $6M seed (Variant, Quantonation) and a $20M Series A (Castle Island, Coinbase Ventures, Balaji) at a $120M valuation.

Strongpoint • 7 Oct 2026

Post-quantum custody for institutions, production in Q4 2026. Partners: Zcash Foundation, Quantus (support from Q1 2027), insurer Relm (20 Oct).

Q-Day Prize

April 2026: 1 BTC paid for breaking a 15-bit ECC key on a cloud quantum computer. Bitcoin keys are 256-bit, but the record is climbing (6 bits in 2025).

Not confirmed

JPMorgan and CME as Strongpoint partners: **not found** in any release or coverage. We dropped this claim from the source documents.

Sources: Series A • Strongpoint • Quantus × P11 • Relm • Q-Day Prize

REFUGE • HOW WE CHOSE

Five tests of a good refuge

1

PQ by default

Every address protected from day one, no opt-in. An option nobody uses saves nobody.

2

Consensus without ECC

In PoS, validator keys on elliptic curves can be stolen to seize the chain. Hash-based PoW has no such keys.

3

Years in production

New crypto breaks in the implementation, not the math. Years without a break matter.

4

External audits

Who reviewed the signature code, when, and what they found. No audit means only promises.

5

Liquidity

A refuge is useless if you cannot get in. How much money trades daily and where.

The PoS trap: if a chain runs on elliptic keys, the attacker steals other people’s stake and signs fake blocks. Then even your post-quantum account is only as safe as that consensus.

Sources: LayerQu • Algorand PQ • NEAR PQ

REFUGE • TOP 5

If Bitcoin breaks tomorrow: five refuges

Chain	PQ by default	Consensus	In production	Audits	24h volume
1. QRL	**yes** • XMSS	PoW, no keys	8.3 yrs (Jun 2018)	Red4Sec, X41, Halborn, Trail of Bits	~$95K
2. Abelian (ABEL)	**yes** • lattice	PoW, no keys	4.5 yrs (Apr 2022)	none found	~$52K, MEXC only
3. Quantus (QTC)	**yes** • ML-DSA (FIPS 204)	PoW, no keys	6 weeks	Neodyme, Eiger, Hashcloak, Immunefi	~$8.4M
4. Algorand (ALGO)	**no** • opt-in Falcon	Ed25519 + EC-VRF	~7 yrs; Falcon accounts since Nov 2025	Falcon code: none found	~$73M, Coinbase
5. Mochimo (MCM)	**yes** • WOTS+	PoW, no keys	8.3 yrs (Jun 2018)	none found	~$3.5K

Algorand is the exception: opt-in protection and an elliptic consensus. It is listed as the “liquid lifeboat”: it is the only one that can carry millions of dollars today.

Sources: QRL • Abelian • Quantus • Algorand • Mochimo • prices

REFUGE • REASONS

Why this order

1 • QRL

+ The only one with all three: default protection, 8 years without a crypto break, named auditors.
– ~$95K daily volume, stateful signatures, a big migration to QRL 2.0 ahead.

2 • Abelian

+ Lattice by default, 4.5 years live, optional privacy.
– Custom, non-standard crypto with no external audit, one exchange, no hardware wallet.

3 • Quantus

+ NIST standard everywhere, even node-to-node; most audits; the only PQ coin with real volume.
– 6 weeks of history, team holds the upgrade key, weak finality, trading runs through NEAR on classical crypto.

4 • Algorand

+ Liquidity (~$73M a day, Coinbase) and live Falcon accounts.
– Opt-in only, elliptic consensus: stolen stake threatens Falcon accounts too. A stopgap.

5 • Mochimo

+ WOTS+ hash signatures by default since 2018.
– No audit, no liquidity (~$3.5K a day). A refuge on paper only.

Bottom line

No chain today combines default protection, years of production, audits and deep liquidity. You would have to move early and in small size.
[CONCLUSION]

Sources: QRL/LayerQu • Abelian/LayerQu • Quantus • Algorand • Mochimo/CMC

REFUGE • WRONG ANSWERS

Often called “quantum-safe”, but not

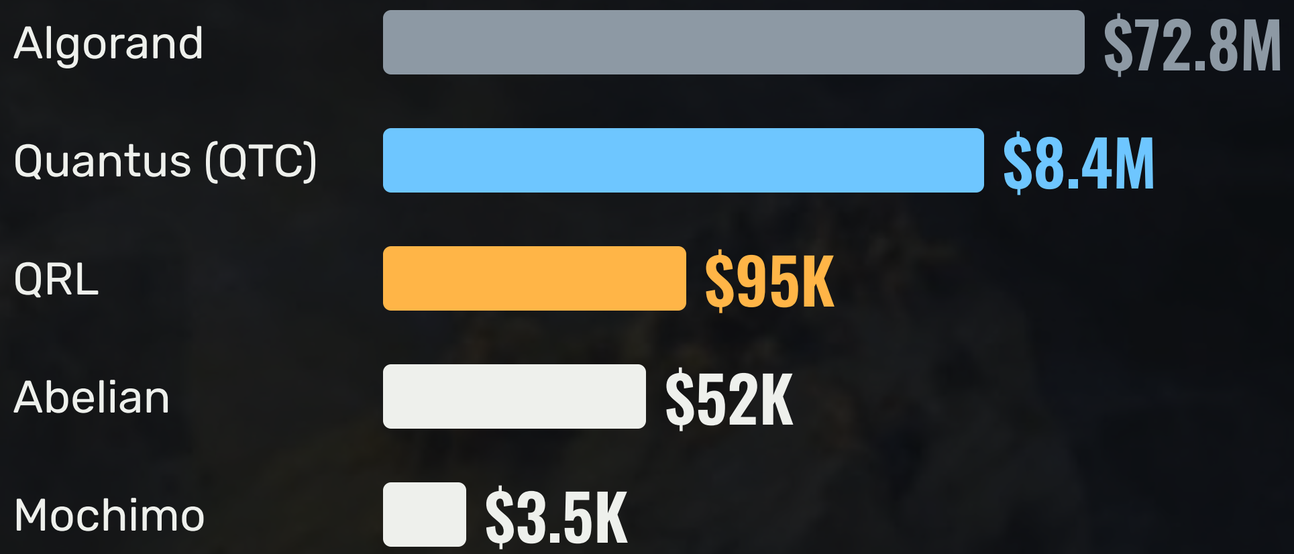
Coin	Why it is not a refuge
NEAR	ML-DSA keys since 20 Jul 2026, but opt-in: **0** of 3,957 sampled signatures were PQ. Validators on Ed25519.
QANplatform (QANX)	Mainnet **not live**. The token on exchanges is ERC-20/BEP-20, i.e. ECDSA.
Cellframe (CELL)	Its own chain supports Dilithium and Falcon, but exchanges trade the ECDSA token.
Algorand	“Falcon in consensus since late 2025” is **false**. Falcon is in State Proofs and opt-in accounts; consensus is Ed25519.
Hedera • ICP • IOTA	No PQ signatures live. Hedera’s “quantum resistance” is just SHA-384 hashing.
Zcash	No PQ signatures yet, target January 2027. ~70% of ZEC sits in the transparent pool.
Nervos CKB • Starknet	CKB: an audited SPHINCS+ lock, but opt-in. Starknet: PQ proofs, classical accounts.
Gold PAXG / XAUT	Also ECDSA ERC-20s. But the issuer knows holders and could reissue legally **[HYPOTHESIS]**

Sources: NEAR/LayerQu • QAN • Cellframe • Algorand • Hedera • Zcash • CKB

REFUGE • REALITY CHECK

The refuge exists, the doors are narrow

24h trading volume, log scale (22 Oct 2026)



$7.5K
QRL order-book depth on MEXC within ±2%. A $100K buy would move the price several-fold

<$10M
a day for all default-PQ coins combined, a rounding error next to bitcoin

The doors run on ECC too
Exchanges and bridges (including NEAR Intents for QTC) run on classical crypto. In a panic they shut first.

Sources: CoinGecko QRL • CoinGecko QTC • CoinGecko ABEL • Coinbase ALGO • CMC MCM • Coinlore

QRL • IN ONE MINUTE

QRL: the veteran of quantum defence

Quantum Resistant Ledger is the first blockchain to protect **every** address with XMSS hash signatures from launch. It runs Proof of Work; the foundation is in Zug, Switzerland. It is now building QRL 2.0 “Zond”: smart contracts, PoS and ML-DSA signatures. The genesis block reads: “the sleeper must awaken”.

$1.24
price, 22 Oct 2026

$96.9M
market cap, ~#298

~$130M
FDV on all 105M QRL

$95K
24h volume

$3.87
all-time high (8 Jan 2018)

2018
XMSS mainnet (26 June)

Sources: CoinGecko • CoinStats ATH • QRL 8 years • QRL 2.0 • tokenomics

QRL • REVENUE AND PRODUCTS

No business yet: a chain and a 2.0 promise

No revenue

No financials or commercial income disclosed. The chain pays miners ~1,865 QRL a day (≈$0.83M a year): inflation, not revenue. Fees are under $1 a day.

~134
transactions a day

173
active addresses a day

19,533
holder addresses

What QRL 2.0 adds

Smart contracts (QRVM, Hyperion language), staking and an EIP-1559 base-fee burn. Plus Chainalysis KYT since 24 Aug 2026, which large exchanges require. The foundation's goal: become home for assets fleeing vulnerable chains.

Checking the "products" in the source doc

Claimed	What we found
PQAS "attestation service"	not found
Ephemeral messaging	draft since 2018, not a product
Quantum Future Ltd "commercial arm"	company dissolved 1 Jun 2021
Consulting	no revenue found
Notarisation, file signing	exists, as free tools

Sources: Quantascan • tokenomics • KYT • Companies House • QIP-008

QRL • TECHNOLOGY

How QRL's protection works

XMSS in plain words

Each QRL address is a **book of one-time stamps**. All stamp fingerprints are combined into a Merkle tree whose root is the public key. Each send uses one stamp. Reusing one leaks the secret.

Pros

Relies only on hash functions, the most conservative defence. Tiny public key (68 bytes). 8 years without a crypto break.

Cons

The wallet must track used stamps. Signature cap per address: 1,024 at the default tree height. NIST approves XMSS only for niche use.

QRL docs ↗ • NIST SP 800-208 ↗

Size is the price of safety

Scheme	Type	Key	Signature
XMSS (QRL 1.x)	hash, stateful	68 B	2,500 B
ML-DSA-87 (QRL 2.0)	lattice	2,592 B	4,627 B
Falcon-1024	lattice	1,793 B	1,462 B
SLH-DSA (SPHINCS+)	hash, stateless	64 B	29–50 KB
ECDSA (BTC/ETH)	elliptic, breakable	33 B	~71 B

A post-quantum signature is 35–700× larger than Bitcoin's. That makes such chains heavier to store.

Sources: Project Eleven registry • liboqs Falcon • liboqs SLH-DSA • QRL 2.0

QRL • AUDITS

Who audited QRL and what they found

2018 — **Red4Sec** ↗
7 weeks, whole stack except PQ crypto: 67 issues (6 critical in the node), all fixed.

10.09.2018 — **X41 D-Sec** ↗
Review of the PQ cryptography itself (XMSS, qrllib).

06.2022 — **Exploit** ↗
Consensus bug: a second coinbase minted 25M QRL. The balance was zeroed by hand; the attacker kept 322.9 QRL.

03.04.2026 — **Halborn** ↗
Two ML-DSA libraries: 13 findings, all informational. Production XMSS was not in scope.

04.08.2026 — **Trail of Bits** ↗
go-qrllib (XMSS + ML-DSA): 1 High, 4 Low, 10 Informational, all fixed.

09.2026 — **Ledger & Release Verifier** ↗
Ledger app audit (11 Sep) and release-verifier audit (18 Sep), no critical issues.

~60%
of QRL 2.0 audits done (16 Oct 2026)

Compared

Abelian and Mochimo: no external audits found. Quantus has more audits but younger code. QRL has the longest record.

Takeaway

The XMSS math never broke. The risk is in implementation and the 2.0 migration, as the 2022 bug and the Trail of Bits finding show.

Sources: QRL weekly 16.10 • ToB PDF • Halborn report • QRIndex

QRL • TEAM

A quantum blockchain run by two doctors



Dr Peter Waterland

Founder, developer

X: @petewaterland ↗

A surgeon by training, following Bitcoin since 2012. Wrote the prototype node and whitepaper in 2016. Administrative role only since Dec 2023.

Dr Iain Wood

Operational manager

no personal X found

General practitioner, ~25 years in the British Army, adviser to a NATO commander. De facto lead since Dec 2023.

Kaushal Kumar Singh

Core developer

no personal X found

Blockchain, big data and ML, high-frequency trading background. Google Protobuf contributor.

Dr Joseph Kearney

Technical advisor

no personal X found

~10 years in blockchain and quantum crypto, PhD “Quantum Advantage on Blockchain Technologies” (Kent). Worked with Project Eleven.

Jack Matier

Director of communications

no personal X found

Linux sysadmin, in IT since 2003.

Ryan Malinowski

Director of advocacy

no personal X found

Ex-head of marketing at an Inc 5000 company, blockchain consulting at Renowned & Co.

No personal X accounts are listed; the official account is @QRLedger ↗. Open source: 65 contributors, 80 repositories. Waterland’s photo is from X @petewaterland (account not confirmed by QRL).

Sources: theqrl.org/team • Peter • Iain Wood • Next chapter

QRL • ROADMAP

QRL 2.0 “Zond”: well advanced, no date

2022	Q1 2024	Q1 2025	31.03.2026	in progress	TBD	TBD
Devnet	Beta testnet	Testnet V1	Testnet V2	Testnet V3	Release Candidate	Mainnet 2.0

What Zond is

PoS with 60 s slots, ML-DSA-87 and Falcon-1024 signatures, the EVM-compatible QRVM and the Hyperion language (a Solidity fork). A testnet validator needs 40,000 QRL, not 2,000 as the source doc said.

Migration

Old XMSS signatures will be verifiable inside QRL 2.0 (a precompile and xmssverify). A rehearsal ran on a 1.62M-block archive.

Partners and collabs

Chainalysis KYT (24 Aug 2026), a University of Manchester grant for new PQ signatures (15 Oct 2026), member of PQCA (Linux Foundation) and the PKI Consortium, Ledger wallet. **QRL is not in the Quantum Alliance.**

Dates have slipped

In Oct 2024 PoS was promised for Q1 2025. It has slipped ~2 years, and the team gives no mainnet date: “not yet set”.

Sources: theqrl.org/2 • roadmap • Testnet V2 • staking • Manchester • weekly 09.10

QRL • TOKENOMICS

105M QRL: no VCs, no unlocks



52 M
2017 sale

13 M
Foundation reserve

14.91 M
Mined so far

25.09 M
Still to mine (~200 yrs)

ICO May 2017

52M QRL at ~$0.08, raised ~$4M. That is 15× in dollars today but only ~0.46× against BTC.

Inflation ~0.85% a year

~1,865 QRL a day to miners. No halvings, a smooth decay. PoS issuance for 2.0 is unpublished.

No unlocks

No VC rounds, no team vesting schedule. The foundation holds 8.45M QRL (10.6%) and, on-chain, has not sold them.

How many circulate?

Three answers: 79.91M (on-chain), 78.39M (CoinGecko), 70.92M (QRL site, ex-reserve). The source doc's "79.5M" is roughly right.

Sources: tokenomics • Quantascan supply • ICO • CoinGecko • rich list

QRL • WHALES AND EXCHANGES

Coins sit with whales, trading on one exchange

31%
held by top 10

65.6%
held by top 100

0.979
Gini coefficient (Bitcoin ~0.88)

136
whales hold 54.8%

Where it trades

Exchange	Share	Note
MEXC	68–74%	also #2 holder: 4.05M QRL (5%)
Biconomy	16–21%	—
XT.com	~10%	flagged inactive, price outlier
Binance • Coinbase • Kraken	0	none; no “Binance delisting” found
DEX	0	no pools

Risks

- One exchange does ~70% of volume
- Price follows quantum headlines, not usage
- 1.x → 2.0 migration means new code
- In 2022 a bug already needed manual intervention
- Rivals and BTC/ETH upgrades may steal the narrative

Sources: Quantascan distribution • rich list • CoinGecko • Coinlore • 2022 post-mortem

QRL • CHART

What news moved QRL

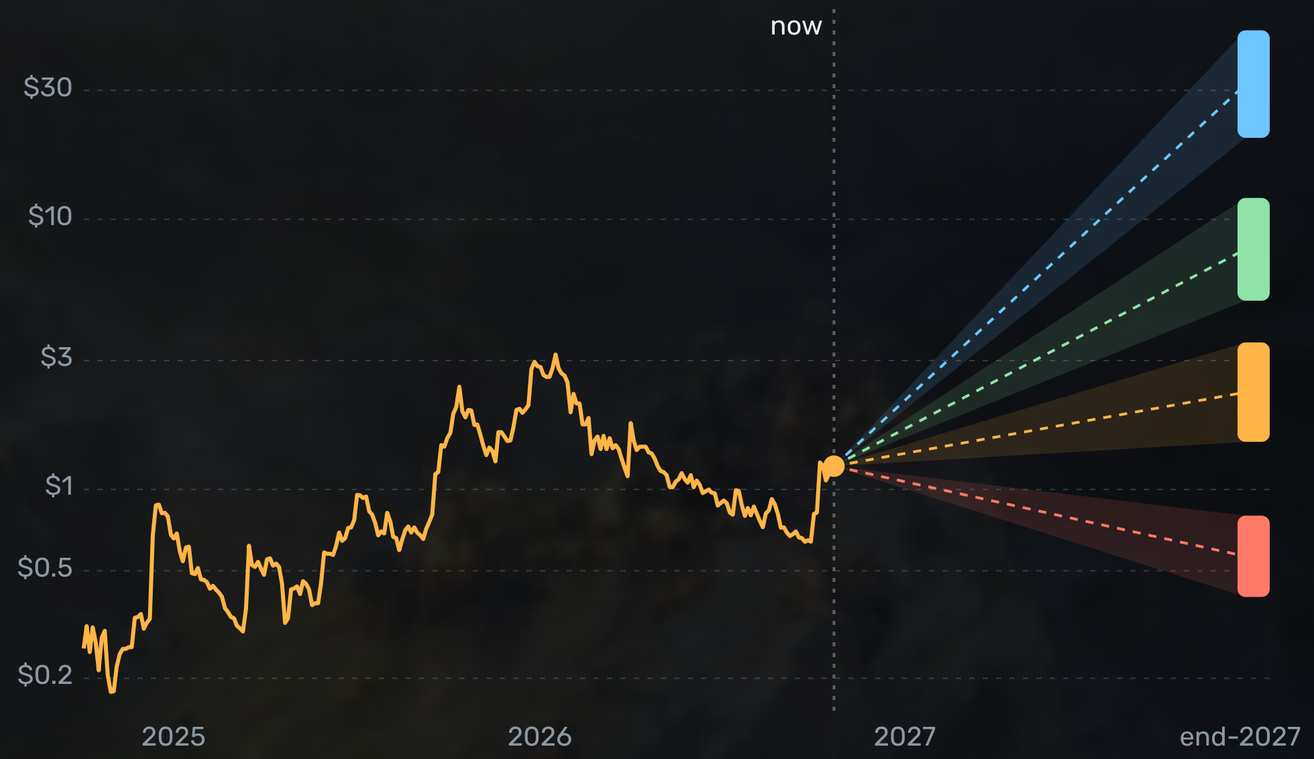


1. **9 Dec 2024** Google Willow chip: +170% in a day ($0.33 → $0.89)
2. **May–Jun 2025** BlackRock adds quantum risk to its ETF prospectus: +33%
3. **Sep–Oct 2025** testnet and quantum narrative: $0.66 → $2.46
4. **10–20.10.2025** market-wide crash → $1.57
5. **16–26 Dec 2025** Saylor vs Edwards quantum debate → $3.24 **[HYPOTHESIS]**
6. **31.03.2026** Google paper names QRL + Testnet V2: +50% in a day
7. **Apr–Sep 2026** no mainnet date → $0.62
8. **1–8.10.2026** +98% with no news: the Quantus/NEAR wave **[HYPOTHESIS]**
9. **15.10.2026** Manchester grant, 10-year anniversary → $1.22

Sources: coinranking • Willow • CryptoSlate • CoinDesk 01.04 • arXiv 2603.28846

QRL • FORECAST TO END-2027

QRL forecast: four scenarios [HYPOTHESIS]



Bear — 35%

$0.40 – $0.80

Mainnet slips again, the quantum theme fades, price returns to 2025 levels.

Base — 45%

$1.50 – $3.50

One or two more quantum waves like 2025–26. Last cycle's peak close was $3.24.

Bull — 17%

$5.00 – $12

Mainnet 2.0 + a tier-1 listing (KYT is in place). Market cap $0.4–1B.

Q-Day — 3%

$20 – $50+

A real quantum break. Price spikes, but there is almost nowhere to trade.

Now $1.24. Probabilities are our estimate from price history and 2.0 plans, not financial advice. Expected value ≈ $3.5, but the median is nearer $1.5–2: the distribution is skewed.

Sources: coinranking • theqrl.org/2 • CoinGecko

QRL • PRICE VS MARKET CAP

QRL price at different market caps

Based on ~81M QRL circulating by end-2027 (79.9M now + ~0.85% yearly inflation).

Market cap	Price	× vs today	Comparable
$50M	$0.62	×0.5	Sep 2026 low ($0.62)
$100M	$1.23	×1.0	today (~$97M)
$250M	$3.09	×2.5	Dec 2025 peak (~$255M)
$500M	$6.17	×5.0	Abelian ×30
$1B	$12	×10.0	Algorand today (~$1B)
$4B	$49	×39.8	top-50 crypto, needs a Binance listing
$12B	$148	×119.5	the source doc’s “$150” target, ×120

In red: the source doc’s forecast ($50–150). It needs a $4–12B market cap, 4–12× Algorand today. Unrealistic without a real quantum break.

Sources: Quantascan • CoinGecko • Coinbase ALGO

QUANTUS (QTC) • IN ONE MINUTE

Quantus: six weeks old

Quantus Network is a “post-quantum Bitcoin”: its own Substrate chain, GPU mining, every signature NIST ML-DSA from block one (9 Sep 2026). No smart contracts. Trades mostly through NEAR Intents.

$88
price, 22 Oct 2026

$26M
market cap

1.4%
of coins circulate: 295K of 21M

$0.5–1.9B
FDV on 5.75M / on 21M

$8.4M
24h volume

$10 → $186
from the 12 Sep low to the 8 Oct high

Revenue and product

The company earns nothing from the chain: all fees go to miners, no dev tax. Private (wormhole) transfers cost 0.04%: half to miners, half burned. The burn is at most ~0.036% of supply a year. No DeFi, no staking.

Sources: CoinGecko • CoinStats • whitepaper • Asymmetric Jump • KuCoin

QUANTUS • TECH AND AUDITS

The cleanest cryptography of all candidates

ML-DSA in plain words

Security rests on “lattices”: finding the key is like locating a point in a many-dimensional grid from slightly noisy coordinates. A quantum computer cannot do it either. Signatures ~3.3 KB, a transfer ~5–7 KB vs ~100 bytes in Bitcoin.

What else is inside

Node-to-node links use ML-KEM-768. Poseidon2 GPU mining. “Wormhole” private transfers hide the sender–receiver link, not amounts. Reversible transfers and account guardians exist.

Weak spots

Poseidon2 was picked “for ZK efficiency, not quantum resistance” and has ~2 years of analysis. No finality: reorgs up to 100 blocks. Forkless upgrades: the team holds the key.

Docs ↗ • Whitepaper ↗ • FIPS 204 ↗

Audits: more than any PQ coin

Who	What and when
Neodyme	ML-DSA, HD wallet • Dec 2025
Eiger / Equilibrium	PoW, Poseidon2, ZK circuits, runtime • Oct 2025 – May 2026
Hashcloak	threshold ML-DSA for the NEAR bridge • in progress
Immunefi	contest 12–25 Aug 2026, $20K pool, ~65K LOC • “under evaluation”
Lean	formal verification of parts of the ZK circuits

But: the audits table in the docs is empty, and the whitepaper and docs disagree on which audits are finished.

Sources: Wormhole docs • Immunefi • iamuvin • Quantum Alliance post • Bitcoin.com

QUANTUS • TEAM AND INVESTORS

Three people on the team, big names among investors



Christopher Smith

Co-founder, CEO, architect

X: @YuviLightman ↗

Whitepaper author. Previously BitMesh, Lunyr, FactoryDAO, early Bitcoin privacy tools. Hosts the QDay podcast.



Joe Mattia

Co-founder, COO

X: @JoeMattia ↗

COO of Quantus Labs LLC (Wyoming, 1–10 staff).

Jonathan Angle

Communications director

no personal X found

Whitepaper co-author, organiser of the Q-Day conference.



Balaji Srinivasan

Investor, led round 2

X: @balajis ↗

Ex-Coinbase CTO, ex-a16z partner. Also a Project Eleven investor. Spoke at Q-Day on 8 Oct.

Mert Mumtaz

Investor

X: @0xMert_ ↗

CEO of Helius (Solana). On the NEAR Foundation board since 15 Oct, a bridge to QTC's main venue. Photo unavailable.



Babak Nivi

Investor

X: @nivi ↗

AngelList co-founder, well-known angel investor.

Funding: ~$2.42M in two rounds: $1.65M at a $20M valuation and $770K at $100M (led by Balaji). Figures from Foresight News, unconfirmed by the project. FDV today is ~$1.85B, ~18× the second round. Bankless ↗

Sources: Chris Smith • Joe Mattia • Crunchbase • PANews/KuCoin • q.day

QUANTUS • PARTNERS AND PLANS

A chain running on borrowed rails

NEAR Intents • 6–7.10

Main venue: QTC trades on near.com without a CEX listing. Quantus has no exchange of its own (no smart contracts). Next: a threshold ML-DSA bridge.

Project Eleven • Strongpoint

Second partner after the Zcash Foundation. Institutional QTC custody from Q1 2027.

Quantum Alliance • 15.10

Co-founder of a 9-member industry alliance: Keystone, Hacken, Abelian, Midnight and others. A standards body, not a deal with Keystone and Hacken as the source said.

Mining pools

Kryptex (~70% of blocks on 10 Oct), F2Pool since 16 Oct, K1Pool, Suprnova. The Keystone wallet supports QTC.

Coming up

1 Dec 2026: testnet-miner airdrop deadline • Q1 2027: Strongpoint • ML-DSA NEAR bridge • a shielded pool is under discussion. No smart contracts planned.

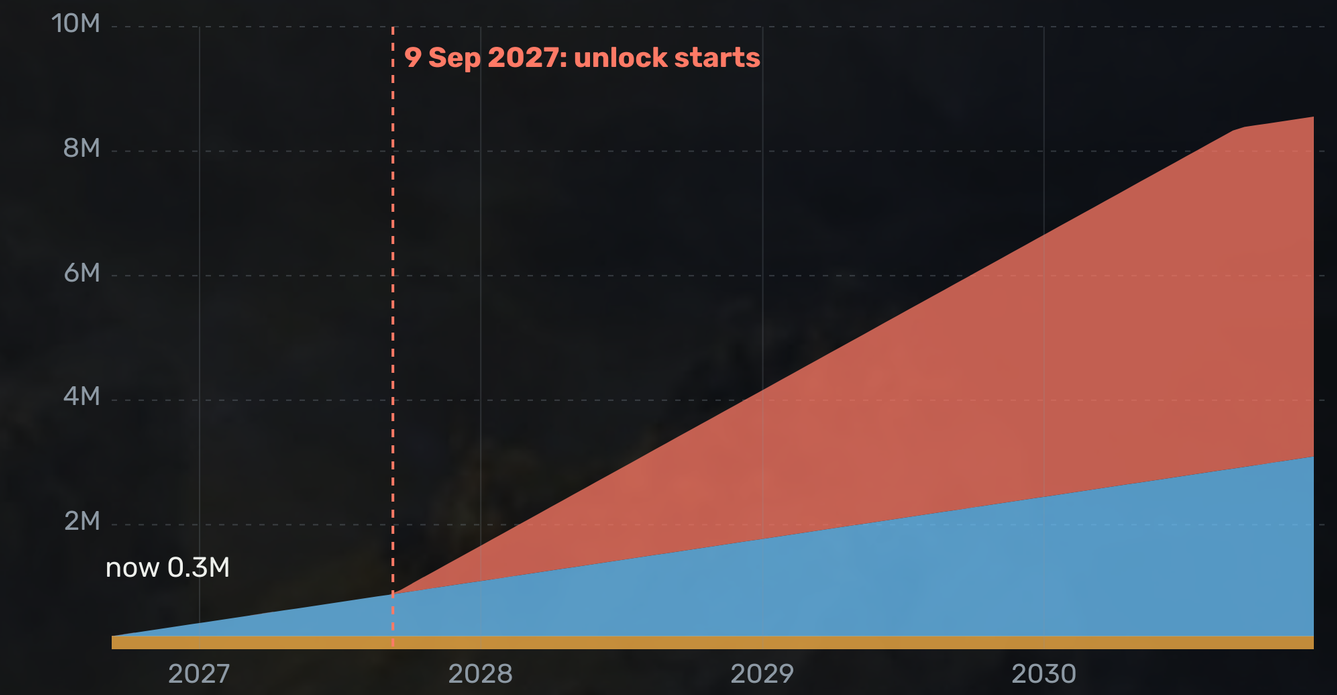
Track record on dates

Mainnet was planned for Q1 2026 and launched 9 Sep 2026, ~6 months late. The “Shared Application SDK” from the source doc was not found.

Sources: TQI • Strongpoint • Alliance • F2Pool • weekly 08.09 • ForkLog

QUANTUS • TOKENOMICS

QTC supply grows ~20× by 2030



- company (210K liquid)
- mined (~1,850/day)
- investor, team, company unlock (5.46M)

21M, like Bitcoin

27% minted at genesis: 23% to investors and team (1-year lock, then 36 months), 4% to the company. Miners get 73%, no halvings.

Inflation ~230% of float

~1,850 QTC a day is 675K a year against a 295K float. From Sep 2027, ~4,950 QTC a day of unlocks join: 2.7× the mining output.

Who holds

The treasury holds 76% of float. On 5 Oct it moved 199,950 QTC to one wallet (likely NEAR liquidity). Mining: one address made 61.6% of blocks (29 Sep), Kryptex ~70%.

Sources: whitepaper • Asymmetric Jump • Phemex • Kryptex • CoinGecko

QUANTUS • CHART

Six weeks of QTC: $10 to $186 and back to $88



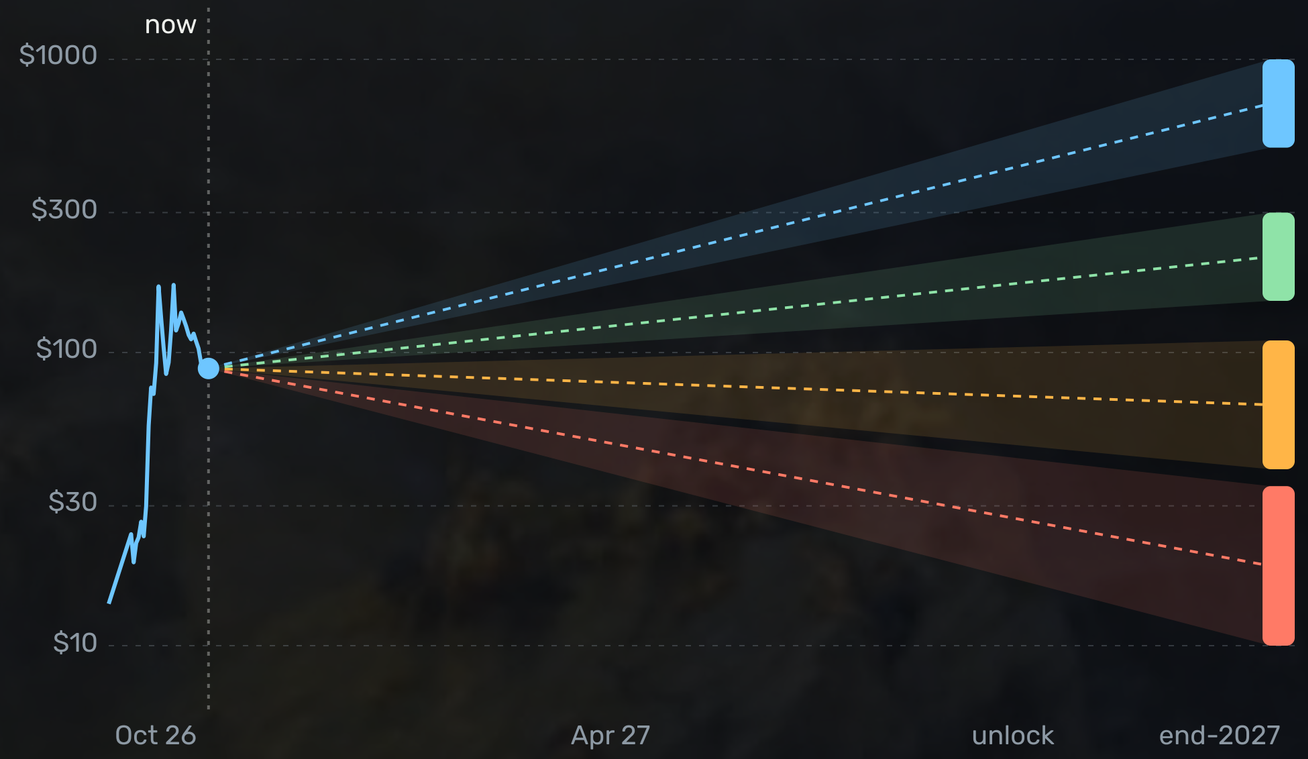
1. **12.09** low of $10.20: only miners have coins
2. **28–29.09** +97% and +140% in two days with no news: a thin SafeTrade book
3. **2.10** $168: +462% since 27 Sep
4. **5.10** treasury moves 199,950 QTC → $84.5
5. **6–7.10** NEAR Intents listing, Bankless piece → $119
6. **8.10** Q-Day conference + Strongpoint: peak $186
7. **9.10** –25% in a day
8. **15–16.10** Quantum Alliance, F2Pool → $111–116
9. **20–22.10** steady decline → $88

Dashed: no data for 13–20 Sep.

Sources: CoinGecko • CoinCheckup • Phemex • Asymmetric Jump • TQI

QUANTUS • FORECAST TO END-2027

QTC forecast: bear is the likeliest case [HYPOTHESIS]



Bear 50%

$10 – $35

Hashrate and interest fade, the Sep 2027 unlock weighs. Price falls to mining cost and below.

Base 35%

$40 – $110

Strongpoint, the bridge and new quantum news waves keep price in October's range.

Bull 13%

$150 – $300

A big CEX listing and institutional demand via Strongpoint. Above the $186 peak.

Panic 2%

$500 – $1,000+

A real quantum break of BTC. But trading via NEAR may halt too.

Now $88. Probabilities are our estimate, weighing the Sep 2027 unlock, ~20× supply growth and the track record of new PoW coins. Not financial advice.

Sources: CoinGecko • whitepaper • Asymmetric Jump

QUANTUS • PRICE VS VALUATION

QTC price at different valuations, end-2027

By end-2027 about 1.66M QTC will circulate (210K liquid + ~0.9M mined + ~0.56M first unlocks), with ~6.56M minted in total. Our calculation.

Valuation	Price if market cap (~1.66M float)	Price if FDV (~6.56M minted)	Comparable
$26M	$16	$3.96	today
$100M	$60	$15	QRL today
$300M	$181	$46	~third of the 8 Oct FDV peak
$1B	$602	$152	Algorand
$5B	$3,012	$762	top-30 crypto
$16B	$9,639	$2,439	source doc's "$2,500" on FDV

In red: the source doc's forecast ($2,500–5,000). On minted coins that is a $16–33B FDV; on all 21M, $52–105B. Top-10 crypto territory.

Sources: whitepaper • CoinGecko • Asymmetric Jump

VERDICT • QRL VS QTC

The veteran vs the rookie

	QRL	Quantus (QTC)
Protection	XMSS (hash) on all addresses since 2018	ML-DSA (NIST) on all addresses since 2026
Track record	**8.3 years**	**6 weeks**
Audits	Red4Sec, X41, Halborn, Trail of Bits	Neodyme, Eiger, Hashcloak, Immunefi
Incidents	2022 bug: 25M QRL, fixed by hand	none yet; 61–70% of blocks from one pool
Supply	**+0.85% a year, no unlocks**	**×20 by 2030, unlocks from Sep 2027**
Liquidity	**~$95K / day**	**~$8.4M / day**
Valuation	$97M (FDV ~$130M)	$26M (FDV $0.5–1.9B)
Main driver	QRL 2.0 mainnet and a listing	Strongpoint, the bridge, quantum news
Our base case	$1.5–3.5 (45%) **[HYPOTHESIS]**	$40–110 (35%) **[HYPOTHESIS]**

Our take: QRL is a time-tested bunker with a narrow door and clean tokenomics. QTC is modern and better armed, but young and facing a mountain of future supply. For a refuge, track record matters more, so #1 is QRL. **[CONCLUSION]**

INTERESTING FACTS

Eight facts you did not know

1. QRL's genesis block reads "the sleeper must awaken".
2. Google's quantum paper (co-authored by Justin Drake and Dan Boneh) names QRL. QRL rose ~50% that day.
3. Google did not publish the attack circuit; it proved it with a ZK proof, after warning the US government.
4. In 2022 a QRL bug minted 25M coins from thin air. The attacker got away with 322.9 QRL, about $65.
5. QTC went $10 → $186 in 26 days. Renting GPUs to mine cost up to $125–170K a day.
6. "QTC" on Gate is Qitcoin, and on SafeTrade it is Qubitcoin. The real Quantus trades there as QUANTUS.
7. Quantus's founder puts the odds of a quantum threat by 2028 at ~50%.
8. The Q-Day Prize record: a 15-bit key. Far from Bitcoin's 256 bits, but in 2025 the record was 6 bits.

Sources: QRL 10 years • arXiv • Forbes • QRL post-mortem • Our Crypto Talk • ForkLog

FACT CHECK

What we corrected in the source documents

Claim in the source documents	Verdict	What is true
Algorand: Falcon in consensus since late 2025	false	consensus is Ed25519; Falcon is in State Proofs and opt-in accounts
JPMorgan and CME partner Strongpoint	not found	partners: Zcash Foundation, Quantus, Relm
QRL in the Quantum Alliance	false	9 members, QRL is not one
QRL validator: 2,000 QRL	false	40,000 QRL on testnet
QRL staking 5–6.5% APR	not found	PoS is not live yet
PQAS, consulting, Quantum Future as QRL revenue	unconfirmed	the company was dissolved in 2021
Quantus: alliance with Keystone and Hacken	partly	it is a 9-member industry body
Quantus: ~1,740 QTC a day	partly	~1,850 a day
Q-Day in 2030–2033	partly	scenarios 2030 / 2033 / 2042
Forecasts QRL $50–150, QTC $2,500–5,000	unrealistic	need $4–33B valuations
Google paper, 6.9M BTC, XMSS since 2018, Quantus ML-DSA	true	confirmed by primary sources

Sources: Algorand • Strongpoint • Alliance • Zond staking • Companies House • Kryptex

WHAT TO WATCH

The quantum race calendar

1 Dec 2026	Quantus: testnet-miner airdrop deadline
Q4 2026	Strongpoint in production; IBM Kookaburra (first fault-tolerant module)
Jan 2027	Zcash: post-quantum payments
Q1 2027	Quantus in Strongpoint; NIST FIPS 206 (Falcon)
2027	QRL: Testnet V3 → RC → mainnet 2.0 (no date)
9 Sep 2027	QTC: unlocks begin, ~4,950 coins a day
end-2027	Algorand: “broad quantum resilience”; NEAR: PQ consensus
2029	IBM Starling (200 logical qubits); Google and Ethereum PQ targets

Warning signs

- old Satoshi-era P2PK coins moving
- a new Q-Day Prize record (above 15 bits)
- a demo of 200+ logical qubits
- BIP-360 or BIP-361 activation

Sources: q.day • Strongpoint • Zcash • IBM • Algorand • FN-DSA

CONCLUSION

A refuge exists. The question is whether you get in

1. A quantum break of Bitcoin is a question of “when”, not “if”. Today the hardware is over 10× short, and Bitcoin can upgrade if it starts in time.
2. The best refuge today is QRL: 8 years of default protection and audits. Quantus is stronger technically but young, with a huge future supply.
3. The doors are narrow: all PQ coins together trade under $10M a day. Preparing for quantum risk means acting early and in small size.

NOT FINANCIAL ADVICE

This review is based on public data as of 22 Oct 2026 and simplified calculations. Forecasts are our hypotheses. Small coins are very volatile: you can lose everything. Make your own decisions.

Questions and ideas for the next reviews: Telegram ↗ • Discord ↗ • X ↗ • qoge.fun ↗