CHAINQUERY.com × LEARNBITCOIN.com

Bitcoin Quantum Exposure

Baseline 2026 Q2

Bitcoin's quantum-exposed supply. Computed genesis-to-tip with STRICT redeem-script parsing. Reproducible to the satoshi.

5,071,264 BTC at risk · 25.3% of supply

Edition	#1
Snapshot date	2026-06-07
Base block height	952,694
Base block hash	`00000000000000000001e505600da6937085fb3e55107af8724ba3802f72a780`
Methodology version	v1.0
Registry size	1,136,306,078 addresses

Executive summary

5,071,264 BTC

at quantum-exposed addresses today.

25.3% of the circulating supply. One bitcoin in four.

ALWAYS-EXPOSED · 21% of pool · 1,063,006 BTC — P2PK, bare multisig, and P2TR: pubkey on chain from the moment the output is created.

REUSE-EXPOSED · 79% of pool · 4,008,258 BTC — Hashed types (P2PKH, P2WPKH, P2SH, P2WSH) where a prior spend revealed the pubkey.

Across 12,749,047 addresses · Snapshot 2026-06-07 · Base block 952,694

The threat is real, the timeline is decade-scale, and Bitcoin has agency. This report is the quarterly anchor for tracking what's currently at risk and, once a post-quantum signature scheme ships on mainnet, for tracking the structural decline of the at-risk pool. Three forces shape the number in any given week. New P2TR outputs add to the always-exposed pool by construction. Reuse on hashed types adds to the reuse-exposed pool. Spends out of either pool to fresh hash-protected addresses subtract from the at-risk total. Ancient P2PK sits dormant. Some of those keys are certainly permanently lost; others are held deliberately by early adopters who are waiting on either a real quantum threat or a real quantum solution before they move. The first ancient P2PK migration will be the most-watched on-chain event in Bitcoin's history; this report exists to track and report on the shift from ECDSA and Schnorr to a post-quantum signature scheme, alongside the migration out of intentionally reused addresses.

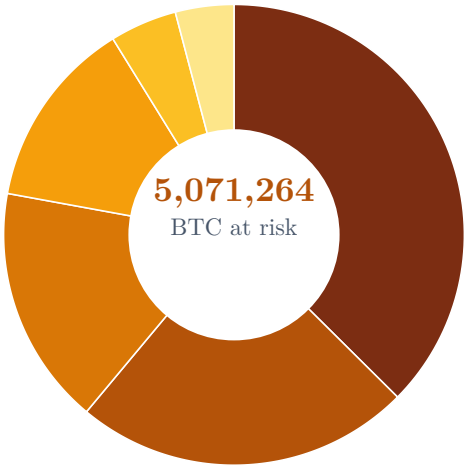
Key findings

- **The largest single bucket is not Satoshi.** 1,896,840 BTC sits at reused P2WPKH, not ancient P2PK. See the breakdown.
- **1,822,794 BTC has been exposed for 5+ years.** Dominated by Satoshi-era P2PK coinbase (853,246 BTC always-exposed) and ancient address-reuse stragglers (969,548 BTC reuse-exposed). Pubkeys on chain since 2014 or earlier.
- **Our number is a rigorous lower bound.** ChainQuery: 25.3%. BIP-361: over 34%. The gap is P2SH and P2WSH spends whose revealed scripts do not contain a pubkey. STRICT parsing excludes them; conservative tooling counts them all.
- **Every new P2TR output is always-exposed from block one.** Hashed types are safe until their first spend; P2TR has no such grace period.
- **Patoshi-era P2PK is the most concentrated cohort in the at-risk set.** 22,223 addresses (0.17% of at-risk addresses) hold 853,247 BTC (17% of at-risk supply). Average balance 38 BTC per address vs 0.4 BTC across the full at-risk pool. Roughly 97× the per-address concentration.

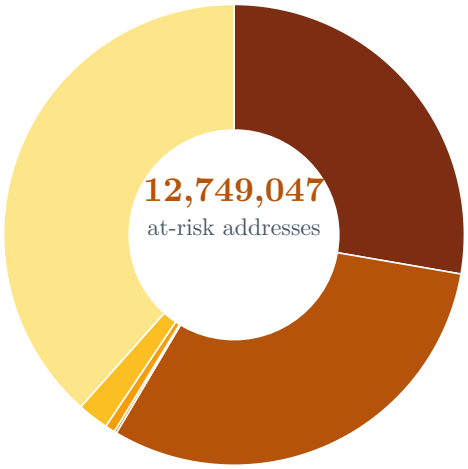
The breakdown

Six buckets, ordered by BTC at risk. **Where the BTC lives** on the left (each wedge is that script type's share of the at-risk BTC). **Where the addresses are** on the right (each wedge is that script type's share of the at-risk address count). When the same script type makes a big slice in one wheel but a tiny sliver in the other, concentration is at work.

Where the BTC lives



Where the addresses are



Same numbers, as horizontal stacked bars:

P2WPKH reuse-exposed
P2PKH reuse-exposed
P2PK always-exposed
P2WSH reuse-exposed
P2SH reuse-exposed
P2TR always-exposed

The largest single bucket is not Satoshi. 1,896,840 BTC is currently held at **P2WPKH** (modern native-segwit) addresses that have been reused at least once. That is 37.4% of the at-risk pool, the editorial pivot of the entire dataset. Reuse-exposed legacy and segwit hashed types together dwarf the ancient P2PK supply: this is users today, not a museum piece.

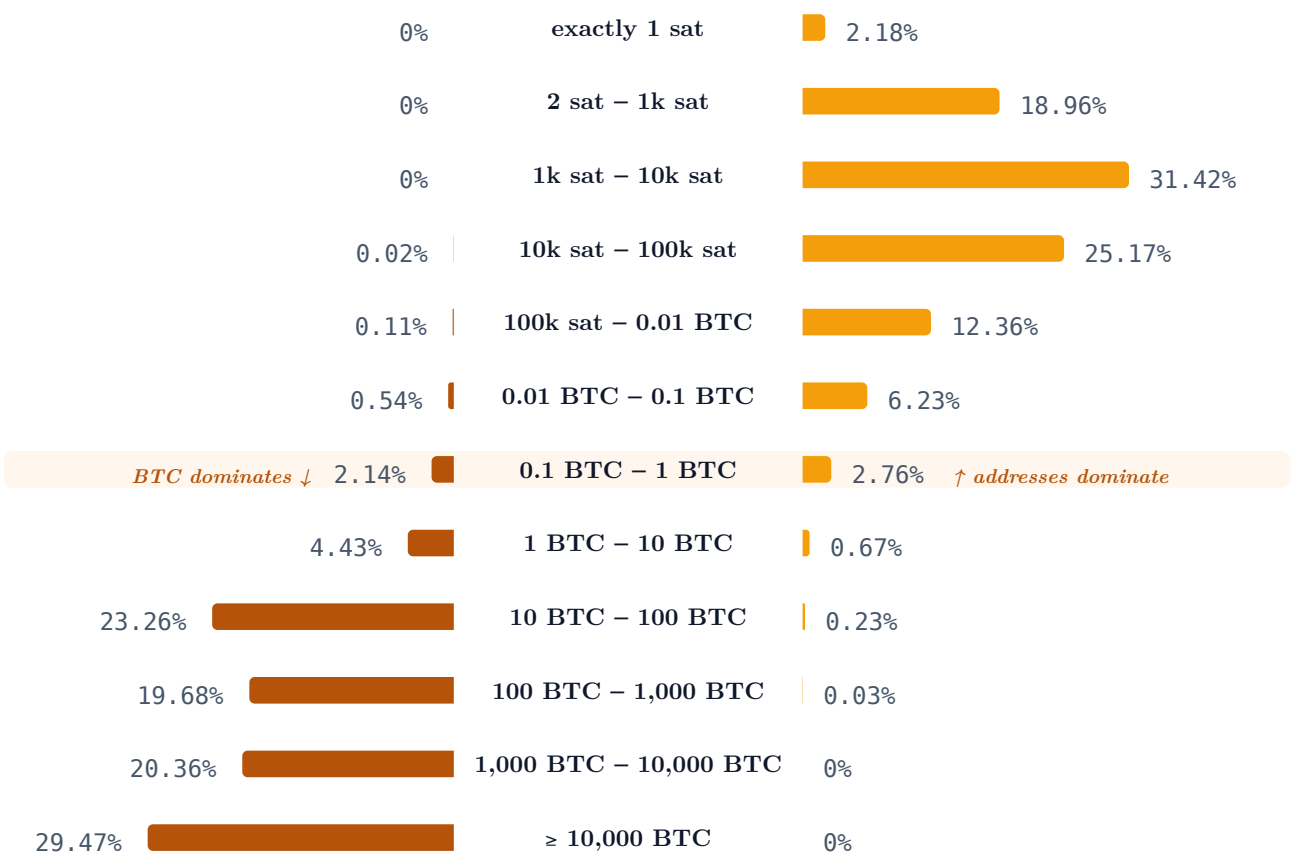
Every new taproot output is exposed at creation time, by design. P2TR (BIP-341) uses the x-only tweaked pubkey directly as the bech32m address. There is no hash layer in front. Every new P2TR output adds to always-exposed supply the moment it lands on chain. Coins leave that pool only when they're spent to a non-always-exposed script type.

P2PK: tiny by entries, huge by BTC. 22,223 addresses (0.17% of at-risk) hold 853,247 BTC: 16.8% of at-risk supply. Average ≈38 BTC per address; ≈896× P2TR's average in the same always-exposed category, and ≈97× the pool-wide average.

Balance distribution

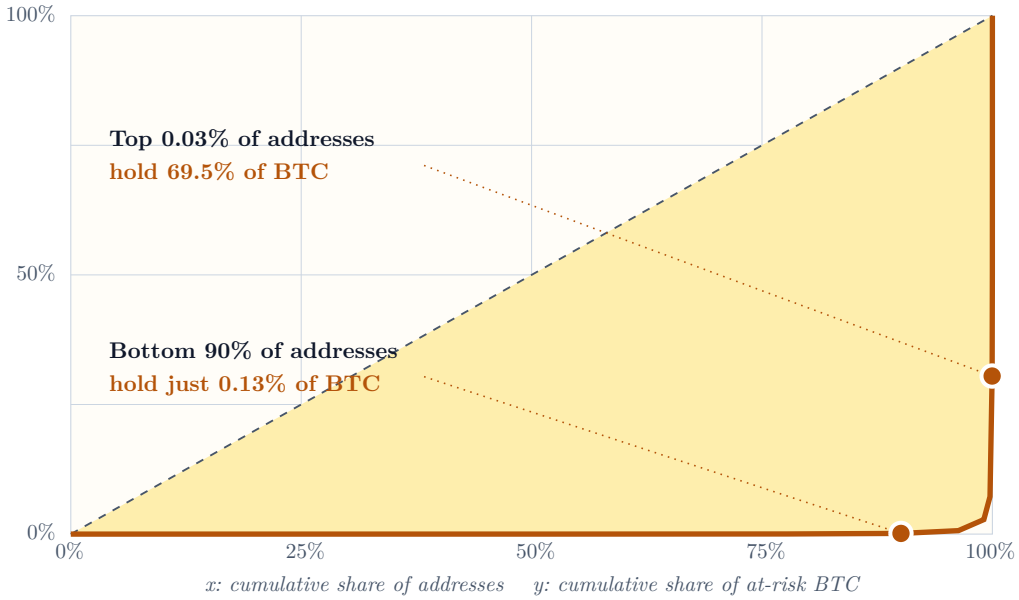
At-risk addresses grouped by current balance. BTC share runs leftward from the bucket label, address-count share runs rightward, both at the same 0-100% scale. The crossover row (highlighted) is where the two are balanced: above it addresses dominate, below it BTC dominates.

Of the 12,749,047 at-risk addresses, ***277,394*** *currently hold exactly 1 satoshi, 2,694,209 hold under 1,000 sats, and 11,484,229 hold under 1M sats.* ***Dust dominates by count; whales dominate by value.***



Concentration curve

How concentrated the at-risk pool is, plotted as a Lorenz curve. X-axis = cumulative share of addresses (sorted smallest balance to largest); y-axis = cumulative share of at-risk BTC. The dashed diagonal is perfect equality (every address holds the same). The further the curve bows toward the bottom-right corner, the more concentrated the holdings. The **Gini coefficient** summarises the bow in one number, from 0 (equal) to 1 (one address holds everything).



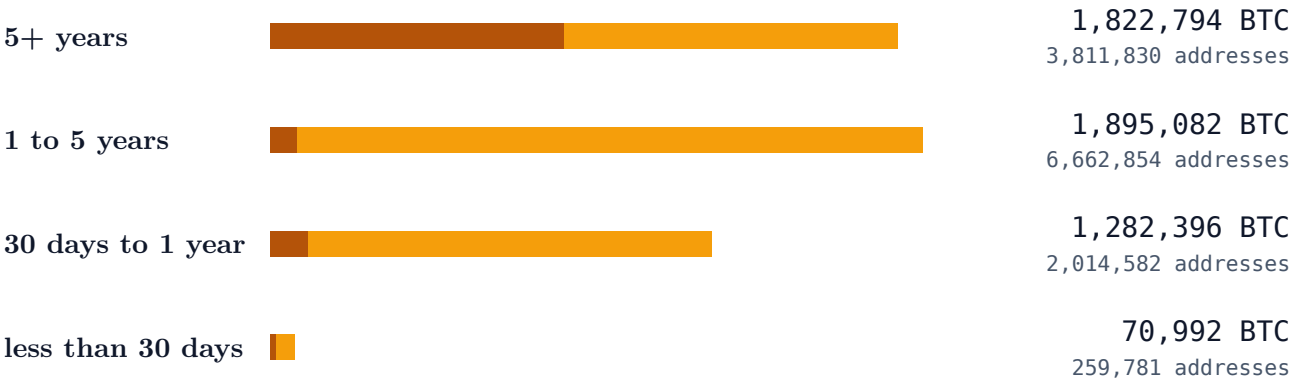
Gini coefficient = 0.997. Concentration is severe: the bottom 90.1% of at-risk addresses hold only 0.13% of at-risk BTC, and the top 0.03% of addresses hold 69.5% of BTC. A perfectly equal distribution would have Gini 0; a single-address monopoly would have Gini 1.

Exposure by age

Of the currently at-risk supply, how long has each address been exposed? Age is base block height minus first-reveal block height, in days. The 5+ year bucket is dominated by Satoshi-era P2PK and ancient address-reuse stragglers: coins that have been forensically reachable for the entire modern history of the network.

Age bucket	Always-exposed	Reuse-exposed	Total
5+ years	853,246 BTC	969,548 BTC	1,822,794 BTC
1 to 5 years	80,154 BTC	1,814,928 BTC	1,895,082 BTC
30 days to 1 year	111,612 BTC	1,170,784 BTC	1,282,396 BTC
less than 30 days	17,994 BTC	52,998 BTC	70,992 BTC

Stacked bar: **deep orange** = always-exposed, **light orange** = reuse-exposed. Width is proportional to the largest bucket's total.



The 5+ year always-exposed slice maps tightly onto the coinbase outputs mined under what is now called the **Patoshi pattern**: a single early miner whose ExtraNonce fingerprint identifies roughly 22% of all blocks in Bitcoin's first year. The deep dive on who's in that slice lives at chainquery.com/stories/patoshi-pattern.

Top 20 exposed addresses

The twenty currently-held addresses whose public key is already on chain, ordered by balance. These twenty sit within the top 40 of the global rich list; the rest of the top 40 are in the hash-protected pool because their pubkey has never been revealed on chain. All twenty here are reuse-exposed (modern hashed types where a prior spend put the pubkey on chain), which is why the script type alone identifies the exposure class. First-reveal height marks the block at which the address's pubkey first appeared on chain.

Address	BTC	Script type	Revealed
bc1ql49ydapnjafl5t2cp9zqpjwe6pdgmxy98859v2	140,063	P2WPKH	788,996
bc1qgdjqv0av3q56jvd82tkdjpy7gdp9ut8tlqmgrpmv24sq90ecnvqqjwvw97	130,010	P2WSH	615,679
bc1qjasf9z3h7w3jspkhtgatgpyvvzgpa2wwd2lr0eh5tx44reyn2k7sfc27a4	96,936	P2WSH	756,372
bc1qd4ysezhmypwty5dnw7c8nqy5h5nxg0xqsvaefd0qn5kq32vwnwqqgv4rzr	91,850	P2WSH	745,096
1Ay8vMC7R1UbyCCZRVULMV7iQpHSAbguJP	72,317	P2PKH	761,392
bc1q0ymzksy046tv4z88ts5nmu7s574umnwmdev3rt	62,658	P2WPKH	911,024
3MgEAFWu1HKSnZ5ZsC8qf61ZW18xrP5pgd	55,905	P2SH	768,281
bc1qws342rlkhszh58rtn35zrw7w076puz83gkcufy	42,660	P2WPKH	916,157
bc1q0j55cut9nd2c88tnnsfultdx696c8lt6n4n0su	42,563	P2WPKH	939,432
bc1q4j7fcl8zx5yl56j00nkqez9zf3f6ggqchwzzcs5hjxwqhsgxvavq3qfgpr	42,399	P2WSH	829,317
bc1qa2eu6p5rl9255e3xz7fcgm6snn4wl5kdfh7zpt05qp5fad9dmsys0qjg0e	38,194	P2WSH	850,318
bc1qy3uw2kk45uj9vsy52rjfhydm2tnd6hreu8vha3	37,484	P2WPKH	910,897
bc1qx9t2l3pyny2spqpqlye8svce70nppwtaxwdrp4	31,643	P2WPKH	639,966
12ib7dApVFvg82TXKycWBNpN8kFyiAN1dr	31,000	P2PKH	59,010
bc1q8taf2eca7pn9wu4czt8fgftqm288xtfxdyt33syzxuexxty733xsszghzk	30,800	P2WSH	905,805
bc1q6h2v33qt0jjvpr2hxxtwhtvdvtn086g0n2qu06	30,574	P2WPKH	926,121
bc1qukw69mjxwp30adfqddv6gcyva26laxz562rhlk	30,467	P2WPKH	911,030
3EMVdMehEq5SFipQ5UfbsfMsH223sSz9A9	26,984	P2SH	643,871
bc1qysj2w7xsw09datsy9mt9x50jn7qjd6qde6d66qm3ce0a4y9uzdpqcavdr0	25,337	P2WSH	889,444
15cHRgVrGKz7qp2JL2N5mkB2MCFGLcnHxv	23,600	P2PKH	741,249

*Of the 20 above, ChainQuery's attribution research identifies **11** as known institutional custody: **Robinhood, Bitfinex, Tether, Upbit, Kraken, OKEx, Deribit, Coincheck, Bybit, and Binance Pool**, totalling 743,586 BTC (68.6% of the top-20 balance, 14.7% of all at-risk supply). The remaining 9 are mostly modern bech32 addresses consistent with other exchange cold storage but not yet positively tied to an entity.*

Methodology

Methodology version **v1.0**. Two components produce the headline number: a **chain walker** that builds the master revealed-pubkey registry from genesis to tip, and a **weekly aggregator** that joins the current UTXO set against that registry. Both are version-locked for this edition; the classifier rules below are sufficient for an independent re-implementation against any Bitcoin Core node.

Source

A single Bitcoin Core 28.0.0 full node, queried via `getblock` with verbosity 3 (which returns each input's prevout `scriptPubKey` plus witness inline) for the master chain walk; weekly aggregates use `dumptxoutset` joined against the master registry.

Exposure rules

Mirroring the BIP-361 threat enumeration:

- **P2PK, bare multisig, P2TR**: always-exposed at output-create time.
- **P2PKH, P2WPKH**: reuse-exposed on first spend (witness contains ⟨signature⟩ ⟨pubkey⟩).
- **P2SH, P2WSH**: reuse-exposed on first spend **if and only if** the revealed redeem script contains a pubkey push followed by a CHECKSIG-family opcode, or contains OP_CHECKMULTISIG / OP_CHECKMULTISIGVERIFY.

A note on taproot script-path spends. A script-path spend reveals the script in the witness but does not add new pubkeys to the registry; the output key was already always-exposed at creation time, so script-path spends are accounting-neutral against the P2TR slice count.

A note on derivation trees. The registry is keyed on specific addresses, not on extended public keys or HD paths. Reusing address `m/0/5` puts its pubkey on chain; the pubkeys at `m/0/6`, `m/0/7`, etc. are derived from the same `xpub` but are not on chain until each is itself reused (or spent at all, in the case of P2TR). A wallet that follows "fresh address per receive" keeps its forward derivation tree in the hash-protected pool until each address is spent for the first time.

A note on Lightning channels. A 2-of-2 funding output is P2WSH. While the channel is open the script is not revealed and the address sits in the hash-protected pool. Cooperative or mutual close reveals `OP_2 ⟨A_pub⟩ ⟨B_pub⟩ OP_2 OP_CHECKMULTISIG`, which the STRICT classifier marks reuse-exposed (CHECKMULTISIG is in the CHECKSIG family under our rules). Routing-only data (HTLC preimages, gossip messages, channel updates) does not affect on-chain pubkey state and does not change the count.

STRICT redeem-script parsing

This is where ChainQuery's number diverges from the published BIP-361 figure. BIP-361 reports **over 34 percent of all BTC** as quantum-exposed. This edition reports **25.3%**. The gap is methodology.

> BIP-361′s conservative count treats every P2SH and P2WSH address whose redeem script was ever revealed on chain as exposed. ChainQuery's STRICT count requires the revealed script to actually contain a pubkey-bearing opcode. Timelock-only redeem scripts (`OP_CLTV OP_DROP OP_TRUE` shapes), hash-preimage scripts, and OP_RETURN-shaped wrappers do not leak pubkeys on spend and are correctly excluded.
>
> **ChainQuery's number is the rigorous lower bound. BIP-361′s is the upper bound that informs the migration framework.** Real exposure sits between these two values; the gap is the

> universe of P2SH / P2WSH addresses whose redeem scripts were revealed but did not actually contain a pubkey. This report will publish that gap explicitly when the data warrants it.

Aggregate

A weekly UTXO-set walk via `dumptxoutset` joins each UTXO from the current snapshot against the master registry; addresses found in the registry contribute their UTXO value to the appropriate exposure slice. The aggregator is a reader, not a writer: the registry itself is kept current by a separate continuous process that appends new reveals at 3-confirmation depth, so by the time the weekly aggregator runs the registry is current within minutes of chain tip. Addresses with zero current balance are excluded, so totals reconcile to "BTC currently at risk" rather than "BTC ever exposed."

Coverage

Methodology version **v1.0** walked **952,695 blocks** covering the entirety of chain history from genesis to base height 952,694. At that height the chain contained approximately **1,372,628,577 transactions** across all script types.

The master `revealed_addresses` registry contains **1,136,306,078 entries** after STRICT exclusion. Each entry is an address whose pubkey is demonstrably on chain in a form usable for ECDSA / Schnorr inversion, regardless of whether that address currently holds any BTC.

The at-risk subset reported on the executive summary and breakdown pages, **12,749,047 addresses**, is the intersection of this registry with the current UTXO set: addresses that are exposed **and** still associated with at least one UTXO with non-zero balance.

The gap between the conservative BIP-361 count and this edition's **25.3%** result is the universe of P2SH and P2WSH spends whose revealed redeem scripts do not contain a pubkey under the STRICT rule: timelock-only redeem scripts (CLTV / CSV gates), hash-preimage scripts (HTLC and atomic-swap shapes), OP_RETURN-shaped wrappers, and any other puzzle-shaped redeem the classifier finds quantum-safe.

Measured reject counts:

Reject category	Rejects	Per block
P2SH spend, revealed redeem contained no pubkey	118,125	≈ 356
P2WSH spend, revealed redeem contained no pubkey	197	≈ 0.6

The two measured categories above are umbrellas over the four conceptual sub-categories named in the preceding paragraph; the current classifier is binary at the script level (pubkey-bearing or not) and does not separately count timelock-only vs hash-preimage vs OP_RETURN-shaped sub-shapes. Coverage is also forward-only at this edition: the reject counter is a chain-tip instrument that landed 2026-05-30, so the totals above span heights **951,699..952,030** (332 blocks, ≈2.5 days). A counting-only backfill walker is planned for the next edition to provide genesis-to-tip totals.

Quarter-over-quarter

This is the **Baseline** edition: no prior edition to compare against. Future quarterly editions will report Δ in total quantum-exposed BTC since the previous edition, per-category Δ (always vs reuse) and per-script-type Δ, movement in the 5+ year aged-exposure bucket, and any methodology-version bumps with line-by-line accounting. Between editions, the web report at chainquery.com/reports/quantum-exposure shows week-over-week Δ continuously.

Threat landscape

The threat is Shor's algorithm, not Grover's. Shor's breaks elliptic curve cryptography given the public key: it derives the private key in polynomial time on a sufficiently large quantum computer. That is the existential exposure, and it is why the 5,071,264 BTC number on the executive summary matters. Grover's gives quadratic speedup on unstructured search; applied to SHA-256 it halves effective security ($256 \rightarrow 128$). Annoying, not catastrophic. Bitcoin's proof-of-work, hashed-but-never-spent addresses, and 21 million supply cap all survive Grover's.

Capability

No cryptographically-relevant quantum computer (CRQC) exists. A CRQC capable of running Shor's against secp256k1 needs millions of stable physical qubits arranged into thousands of logical qubits via error correction, with sustained coherence across millions of gate operations and gate fidelity high enough that error-correction overhead does not blow up. State of the art today is hundreds of noisy physical qubits with demonstrated logical qubit counts in the single digits. Multiple orders of magnitude separate today's systems from CRQC on several axes.

Most expert estimates put a CRQC capable of breaking 256-bit ECDSA in a 10-to-30-year window. BIP-361′s authors cite academic roadmaps pointing at 2027 to 2030; more conservative accounts push to the 2040s or later. The honest planning posture is "before we are ready, and possibly suddenly."

Candidate replacements

NIST finalised two post-quantum signature standards in August 2024: **ML-DSA** (FIPS 204; lattice-based; smaller and faster, less mature) and **SLH-DSA** (FIPS 205; hash-based; larger and slower, more conservative).

The migration framework is split across two drafts. **BIP-360** (Pay-to-Quantum-Resistant) proposes the new address format and the script type that holds a PQ pubkey. **BIP-361** (Post-Quantum Migration) defines the sunset schedule for ECDSA and Schnorr over a multi-year window. Neither BIP picks the underlying algorithm; that lives in a forthcoming separate BIP whose number has not been assigned because the cryptographic choice (ML-DSA vs SLH-DSA vs a classical-plus-PQ hybrid) is still pre-consensus. The TBD BIP number is not a placeholder we are waiting on; it is the literal state of the proposal pipeline.

Reproducibility appendix

This edition was rendered against a verifiable, self-describing snapshot. Anyone running a Bitcoin Core full node can re-derive the headline number to the satoshi from the rules in Methodology and the identifiers below.

Version-locked components

Component	Identifier
Bitcoin Core version	Bitcoin Core 28.0.0 (P2P subversion: `/Satoshi:28.0.0/`)
Base block hash	`000000000000000000001e505600da6937085fb3e55107af8724ba3802f72a780`
Base block height	952,694
Registry built through height	952,847
Registry size	1,136,306,078 addresses
Methodology version	v1.0

Registry-built-through is higher than the base block because the tip-tracker continues to append reveals at 3-confirmation depth after the weekly UTXO aggregation; all headline numbers are computed at the base block.

How to re-derive

Two passes against a Bitcoin Core full node reproduce the headline numbers:

1. **Chronological registry build.** Walk the chain genesis-to-tip via `getblock <hash>` at verbosity 3 (returns each input's prevout `scriptPubKey` plus witness inline). For every output, classify the script type; for every input, parse the witness or scriptSig to determine whether the spend revealed a pubkey under the STRICT exposure rules above. Append addresses whose pubkey first hits the chain in usable form to a registry, with one row per address recording the first-reveal height, the block timestamp, the exposure category (always or reuse), the original script type, and a tag identifying which classifier arm fired.
2. **UTXO-set aggregate.** Take a `dumptxoutset` snapshot at a chosen base block height. For each UTXO, look up its address in the registry; if present, add the UTXO's value to the appropriate exposure slice. Sum by category and script type to produce the per-bucket totals you see in the breakdown.

The RPC call shape:

```
curl -s --user $RPCUSER:$RPCPASS -X POST \
     -H 'content-type: text/plain' \
     --data '{"method":"getblock","params":["<hash>", 3]}' \
     http://<bitcoind-host>:8332
```

Verbosity 3 returns each input's prevout `scriptPubKey` and witness inline, which is what makes the chronological walk possible without random-access UTXO lookups.

Registry schema

```
CREATE TABLE revealed_addresses (
  address                   TEXT PRIMARY KEY,
  first_revealed_height     INTEGER NOT NULL,
  first_revealed_block_time INTEGER NOT NULL,
  exposure_category         TEXT NOT NULL,  -- 'always' | 'reuse'
  original_script_type      TEXT NOT NULL,  -- 'pubkey' | 'pubkeyhash' | ...
  reveal_reason             TEXT NOT NULL
);
```

`reveal_reason` identifies which classifier arm fired. The six values in use are `p2pk_output`, `multisig_output`, `p2tr_output` (for outputs whose script type is always-exposed at creation), `input_spend` (for P2PKH and P2WPKH spends, which always reveal ⟨sig⟩ ⟨pubkey⟩ in the witness), and `p2sh_redeem_reveal` / `p2wsh_redeem_reveal` (for P2SH and P2WSH spends whose revealed redeem script contained a pubkey under the STRICT rule above). The enumeration is exhaustive over the script-type universe and is the authoritative answer to "why does this address appear in the registry?" The distribution across the registry as of this snapshot:

reveal_reason	Entries	Share
input_spend	975,377,153	86.0%
p2tr_output	78,321,195	6.9%
p2sh_redeem_reveal	42,353,150	3.7%
p2wsh_redeem_reveal	35,743,280	3.2%
multisig_output	2,584,301	0.2%
p2pk_output	216,995	0.02%

Input-spend reveals (P2PKH and P2WPKH first spends) dominate by an order of magnitude. P2TR adoption since activation in 2021 has produced the second-largest cohort despite covering only a fraction of the chain's history. The P2PK cohort is tiny by entry count at 0.02% but disproportionately important by BTC: see the breakdown, where the P2PK script-type row still holds **853,275 BTC** across 22,223 addresses, almost entirely early-mining coinbase outputs whose pubkeys have been on chain since 2009-2010.

JSON API

The same data feeding this PDF is available as bulk JSON for programmatic consumers. Endpoints are bearer-gated; browser requests from other origins are blocked. These are server-side endpoints by design.

Access. The dataset is gated and released under a license separate from this PDF; to request an API token, email **hello@chainquery.com**. We encourage research, reuse, and downstream tooling against this data; write to us about what you want to do with it. The default `/api/lists/quantum-at-risk.json` endpoint returns the top 100 currently-held exposed addresses by balance; bulk access to the full at-risk set (≈13M rows) is available on request via the same email.

Endpoint

```
GET https://chainquery.com/api/lists/quantum-at-risk.json
Authorization: Bearer <your-token>
```

Sample request

```
curl -sH 'Authorization: Bearer <TOKEN>' \
  https://chainquery.com/api/lists/quantum-at-risk.json
```

Sample response shape

```
{
  "version": 1,
  "list":    { /* slug, title, blurb, methodology */ },
  "stats":   { "snapshot_date", "exposed_address_count",
               "total_btc_at_risk", "pct_of_supply",
               "is_lower_bound" },
  "entries": [
    { "rank", "address", "balance_btc",
      "exposure_category", "original_script_type",
      "first_revealed_height" },
    /* top 100 by balance; bulk access on request */
  ]
}
```

References

External authorities cited throughout this edition. The order below is by load-bearing weight on the methodology, not numerical order.

Standards informing this work

BIP-361	**Post-Quantum Migration.** Lopp et al. The migration framework this report's methodology contrasts against; the source of the "over 34 percent" upper-bound figure. github.com/bitcoin/bips/blob/master/bip-0361.mediawiki
BIP-360	**Pay-to-Quantum-Resistant.** The address-format draft that pairs with BIP-361′s migration framework. github.com/bitcoin/bips/blob/master/bip-0360.mediawiki
FIPS 204	**ML-DSA (Module-Lattice-Based Digital Signature Standard).** NIST, August 2024. Candidate post-quantum signature scheme. csrc.nist.gov/pubs/fips/204/final
FIPS 205	**SLH-DSA (Stateless Hash-Based Digital Signature Standard).** NIST, August 2024. Conservative hash-based alternative. csrc.nist.gov/pubs/fips/205/final

Foundational references

Shor (1994)	**Algorithms for quantum computation: discrete logarithms and factoring.** The polynomial-time quantum attack against ECDSA and Schnorr. The existential threat this report measures exposure to. ieeexplore.ieee.org/document/365700
Lerner (2013)	**The well-deserved fortune of Satoshi Nakamoto.** The original ExtraNonce-pattern analysis identifying the Patoshi cohort that dominates the 5+ year always-exposed bucket. bitslog.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto

Related Bitcoin Improvement Proposals

BIP-341	**Taproot.** Defines P2TR. The x-only tweaked pubkey is the address; always-exposed by construction. github.com/bitcoin/bips/blob/master/bip-0341.mediawiki
BIP-143	**SegWit transaction signature verification.** Defines the witness structure that makes P2WPKH and P2WSH pubkey reveals visible on spend. github.com/bitcoin/bips/blob/master/bip-0143.mediawiki

Companion materials

LearnBitcoin	**Quantum and Bitcoin.** The rabbit hole. Plain-language explainer with sourced facts. learnbitcoin.com/rabbit-hole/quantum-and-bitcoin
ChainQuery	**Quantum exposure report (web).** The always-current weekly version of this methodology. chainquery.com/reports/quantum-exposure
ChainQuery	**The Patoshi pattern (story).** Deep dive on the cohort that dominates the 5+ year always-exposed bucket. chainquery.com/stories/patoshi-pattern

About this report

ChainQuery.com operates the data infrastructure: the bitcoind node, the chronological chain walk that built the master `revealed_addresses` registry, the weekly UTXO-set aggregation, the always-current report at chainquery.com/reports/quantum-exposure, the JSON endpoints, the tip-tracker that keeps the registry within minutes of chain tip.

LearnBitcoin.com operates the editorial layer: the rabbit-hole at learnbitcoin.com/rabbit-hole/quantum-and-bitcoin that walks readers through the threat in plain terms with sourced facts. No panic, no dismissal. Just the honest version.

License

Attribution string:

```
“Bitcoin Quantum Exposure: Baseline 2026 Q2” by ChainQuery.com × LearnBitcoin.com.
CC BY 4.0. https://chainquery.com/reports/quantum-exposure
```

Academic citation:

```
ChainQuery.com × LearnBitcoin.com (Baseline 2026 Q2). Bitcoin Quantum Exposure Quar-
terly. Snapshot block 952,694, 2026-06-07.
https://chainquery.com/reports/quantum-exposure
```


Next edition

The quarterly cadence is fixed: editions ship on the 15th of January, April, July, and October. The web report at chainquery.com/reports/quantum-exposure stays current weekly between editions. The methodology version is bumped only when the walker or aggregator changes in a way that affects numbers; every change is documented inline in the edition that introduces it.

Quantum is real.

Bitcoin is preparing.

Move your coins to modern addresses.