Note on authorship: "Zipherpunks" is an independent research handle. We are not members of, affiliated with, or endorsed by the original Cypherpunks mailing list, its founders (Hughes, May, Gilmore), or any of the legends who built the cryptographic tools we all depend on. We just read their work, took it seriously, and wrote code instead of asking permission. If that sounds familiar, it should — we learned it from them.
"Cypherpunks write code." — Eric Hughes, 1993. We're trying.

Satoshi's Donation Protocol: Security-Conditional Spendability for Quantum-Vulnerable Dormant Bitcoin

Zipherpunks

April 2026

Abstract

1,720,270 BTC reside in P2PK addresses with public keys exposed on-chain since creation. These outputs rely on ECDSA security assumptions that may degrade under quantum computing. We propose Satoshi's Donation Protocol (SDP): a consensus-layer mechanism that restricts spendability of quantum-vulnerable P2PK outputs created before a fixed cutoff height (block ~1,035,000, approximately January 3, 2028). The restriction activates only once the block subsidy drops below 1 BTC (halving 6, block 1,260,000, approximately 2032). Invalid spend paths are removed; resulting value integrates into block rewards following Bitcoin's existing incentive structure. If no cryptographic break occurs, no additional value enters circulation. Holders in quantum-safe address types (P2PKH with unrevealed keys, P2SH, P2WSH, Taproot, and future post-quantum formats) are never impacted and can hold indefinitely. The 21 million hard cap is never violated. This paper presents the mechanism, its economic trigger, its quantum defense properties, a comparison with prior proposals (PoAR, BIP-361, Freicoin), and a full audit separating verified facts from unproven assumptions.

1. Introduction

In 2010, Satoshi Nakamoto wrote:

> *"Lost coins only make everyone else's coins worth slightly more. Think of it as a donation to everyone."*
>
> — Satoshi Nakamoto, BitcoinTalk, June 2010

That was accurate for a young network with generous block rewards. Bitcoin now faces three problems. 3–4 million BTC are permanently lost[1], reducing effective supply to roughly 17 million. 1,720,270 BTC sit in P2PK addresses[2] with public keys exposed on-chain — vulnerable to Shor's algorithm on a cryptographically relevant quantum computer (CRQC). Timelines range widely: Google targets ~2029 for error-corrected QC, NIST will deprecate ECC by 2030 and disallow by 2035, skeptics say 2040 or later[3]. Breaking secp256k1 needs roughly 500,000 physical qubits (Google, 2025). And the block reward drops below 1 BTC for the first time at halving 6 (~2032).

Satoshi wrote: *"In a few decades when the reward gets too small, the transaction fee will become the main compensation for nodes."*[4] That decade is approaching. Whether fees alone can secure a multi-trillion dollar network is an open question.

We propose Satoshi's Donation Protocol (SDP): a consensus-layer mechanism that restricts spendability of quantum-vulnerable P2PK outputs once their security assumptions can no longer be guaranteed. Invalid spend paths are removed; remaining value integrates into block rewards. Triggered only when the block subsidy drops below 1 BTC. Scoped to P2PK addresses with exposed public keys. Key rotation preserves ownership. This proposal does not assume a specific quantum timeline; it defines a deterministic response if ECDSA assumptions fail for exposed keys. If no cryptographic break occurs, no additional value enters circulation.

2. Prior Proposals

Several proposals have addressed dormant coins or mining incentives. All were rejected or criticized for fundamental design choices:

Table 1. Prior proposals and their limitations.

Proposal	Scope	Criticism
PoAR (2025)[5]	All UTXOs, 20yr	Targets all regardless of crypto status
Issue #31941 (2025)[6]	All UTXOs, 16yr	No quantum justification
Freicoin (2012)[7]	All coins, 5%/yr	Penalizes all holders
BIP-361 (2026)[8]	QC-vulnerable	Freezes, adds nothing to security budget

Each failed on at least one axis: universal scope (no cryptographic justification), no economic trigger, or framing that invites rejection. SDP addresses all three.

3. Mechanism

3.1 Scope: Quantum-Vulnerable Addresses Only

The dormancy clock applies exclusively to UTXOs where the public key is exposed on-chain and can be targeted by Shor's algorithm:

Table 2. Address type eligibility.

Address Type	Key Exposed?	Subject to SDP?
P2PK	Yes — at creation	**Yes (Phase 1)**
P2PKH (reused, key revealed)	Yes — after spend	Phase 2 (future debate)
P2PKH (never spent)	No — HASH160	No
P2SH / P2WSH / P2WPKH	No	No
P2TR (Taproot)	No*	No
Future PQC types	No	No

If your public key is not on-chain, your cryptographic guarantees are intact. Hold forever. Phase 1 targets P2PK only — the cleanest case (public key embedded in scriptPubKey at creation, deterministic detection). Reused P2PKH is deferred to Phase 2, subject to separate community debate.

3.2 Economic Trigger

The donation activates when `GetBlockSubsidy()` returns less than 1 BTC. This occurs at halving 6, block 1,260,000, around 2032. The reward at that point: 0.78125 BTC (50*COIN >> 6). Before this, nothing changes.

3.3 Dormancy Cutoff: January 3, 2028

The cutoff is a fixed block height: ~1,035,000 (approximately January 3, 2028). A fixed cutoff avoids ambiguity, coordination risk, and last-minute chain instability. This provides a multi-year key-rotation window from announcement. Any P2PK UTXO created before this height and not rotated to a quantum-safe address enters the donation pool. Holders have from announcement until halving 6 (~2032) before any donation occurs. P2PK coins from 2009–2012 are already 16–19 years dormant by then.

The 1 BTC subsidy threshold and the cutoff height are proposed starting values. Both are BIP-level parameters subject to refinement through the community process described in Section 11; the whitepaper fixes them only to make the mechanism concretely analyzable.

3.4 Fill-the-Gap Formula (with Donation Halving)

The donation fills the gap between the halving reward and a decaying cap. Like Bitcoin's subsidy, the donation halves every 210,000 blocks. The pool never fully depletes:

```
INITIAL_GAP = 21_875_000  // 0.21875 BTC (1 BTC - halving 6)
donation_halvings = (height - 1_260_000) / 210_000
donation_cap = INITIAL_GAP >> donation_halvings
donation = min(donation_cap, pool / remaining_blocks)

// Halving 6: cap=0.21875 -> donation = 0.21875 BTC
// Halving 7: cap=0.10938 -> donation = 0.10938 BTC
// Halving 8: cap=0.05469 -> donation = 0.05469 BTC
// Halving 9: cap=0.02734 -> donation = 0.02734 BTC
// Asymptotic: donation -> 0 (never depletes)
```

Table 3. Donation halving schedule.

Era	Subsidy	Don. Cap	Total	Pool Used	Pool Remaining
Halving 6	0.78125	0.21875	1.00000	~45,938	~1,674,332 (97.3%)
Halving 7	0.39063	0.10938	0.50000	~22,969	~1,651,364 (96.0%)
Halving 8	0.19531	0.05469	0.25000	~11,484	~1,639,879 (95.3%)
Halving 9	0.09766	0.02734	0.12500	~5,742	~1,634,137 (95.0%)
Halving 10	0.04883	0.01367	0.06250	~2,871	~1,631,266 (94.8%)
Halving 11	0.02441	0.00684	0.03125	~1,436	~1,629,831 (94.7%)
Halving 12	0.01221	0.00342	0.01562	~718	~1,629,113 (94.7%)
13, 14, 15...	halves	halves	halves	halves	converges → 94.7%
Infinite sum				**~91,875**	**~1,628,395 (94.7%)**

At halving 6: 0.21875 BTC/block (~11,497 BTC/year). The geometric sum converges to ~91,875 BTC — 5.3% of the 1.72M pool. 94.7% stays untouched. Same geometric decay as Bitcoin's emission schedule.

3.5 Block Donation Messages

Satoshi put a message in the genesis block: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."* SDP uses the same space. Every block with donated coins carries a structured tag:

```
SDP: 0.21875 BTC donated from 3 QC-risk
dormant UTXOs | Think of it as a donation
to everyone.
```

The coinbase scriptSig supports up to 100 bytes after the BIP-34 height. Every donation is recorded permanently on-chain.

4. Game Theory

Table 4. Impact by holder type.

Holder	Address	Effect	Cost
HODLer (P2PKH/Taproot)	QC-safe	Not impacted	Zero
Active user	Any	No change	Zero
P2PK holder (alive)	QC-exposed	Move to safe addr	~$1–5
Lost keys (P2PK)	QC-exposed	Value flows to security budget	Returned
Early P2PK (incl. Patoshi)	QC-exposed	Same rules as all P2PK; key rotation preserves ownership	Same condition
Quantum attacker	P2PK	Exposure neutralized	Preempted

Key rotation is one transaction to a quantum-safe address. Ownership is preserved forever. This is not revocation — it is a key-rotation deadline with years of advance notice.

4.1 Early P2PK Outputs (Patoshi Pattern)

Approximately 1.1M of the 1.72M BTC in P2PK are attributed to the Patoshi mining pattern. SDP does not target these outputs specifically; it targets a cryptographic condition (exposed public key in scriptPubKey) shared by all 45,257 P2PK UTXOs in the current set[2]. The rule is identical for all. If the keyholder exists, one transaction preserves ownership. If keys are lost, those outputs face the same ECDSA degradation as any other P2PK UTXO. The perception risk is acknowledged: if this is seen as targeting specific outputs rather than a cryptographic condition, the proposal fails politically regardless of technical merit.

4.2 Edge Cases

Mass key rotation before cutoff: desired outcome. Every coin rotated is a coin protected from quantum. The pool size adapts. **Mempool congestion near cutoff:** the cutoff is ~4 years before donation activation; fee spikes from procrastination are self-correcting within blocks. **Miner manipulation:** donation cap is deterministic per block (INITIAL_GAP >> halvings). Miners cannot influence the cap, pool allocation, or extract more than the cap regardless of block ordering. **Strategic inactivity:** the opt-out remains available until the cutoff. Inaction is not a strategy against cryptographic degradation. **Whale coordination:** large P2PK holders rotating simultaneously proves the mechanism works — the problem is solved, the pool is empty.

5. Quantum Defense

P2PK addresses expose the public key on-chain at creation. These coins predate BIP-32 (2012) and BIP-39 (2013). There is no derivation chain. The private key is the root. If ECDSA assumptions degrade, an attacker who derives the key via Shor's algorithm is indistinguishable from the owner. SDP does not assume a specific quantum timeline; it defines a deterministic response if ECDSA assumptions fail for exposed keys.

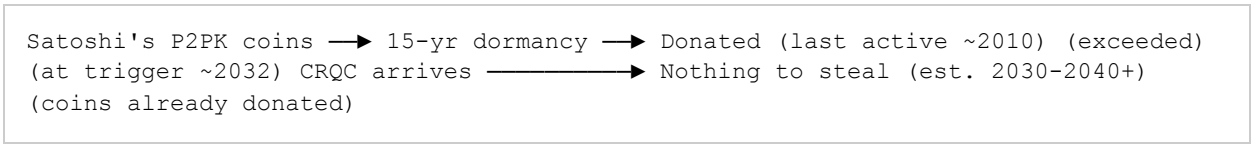

Fig. 1. Quantum timeline vs. SDP donation timeline.

If ECDSA assumptions fail, exposed keys become insecure immediately; until then, they remain valid. If failure occurs, exposed keys face two outcomes: exploited by an adversary, or recycled into the security budget. A reasonable objection asks: why not wait for a demonstrated CRQC? Because once a CRQC exists, every P2PK private key is derivable immediately — there is no post-hoc migration window. The NIST deprecation schedule (ECC deprecated 2030, disallowed 2035) reflects the same logic. SDP's fixed cutoff provides a predictable deadline. If quantum never arrives, the pool sits unused. The mechanism is a contingency, not a prediction.

6. Satoshi Alignment

If this contradicts what Satoshi wrote, it does not belong in Bitcoin:

Table 5. Alignment with Satoshi's quotes.

Quote	Source	Fit
"Lost coins...donation to everyone"	BitcoinTalk, 2010	100%
"Incentive can transition entirely to transaction fees"	Whitepaper, Sec. 6	100%
"In a few decades when the reward gets too small"	BitcoinTalk, 2010	95%
"Any needed rules and incentives can be enforced"	Whitepaper, Conclusion	100%
"Cryptographic proof instead of trust"	Whitepaper, Sec. 1	100%
"No central authority to issue them"	Whitepaper, Sec. 6	100%
"Core design was set in stone"	BitcoinTalk, 2010	80%

"Set in stone" meant the core design: 21M cap, proof-of-work, no trusted third party. SDP preserves all of these. Satoshi modified Bitcoin after v0.1 — 1MB limit, OP_NOP codes, alert system. His conclusion leaves room for new rules: *"Any needed rules and incentives can be enforced with this consensus mechanism."*

He did not anticipate quantum computers threatening 1.72M BTC in P2PK addresses. That problem did not exist in 2008.

7. Cypherpunk Alignment

No cypherpunk has advocated seizing dormant digital property. SDP does not revoke ownership. Spendability is conditional on cryptographic security assumptions. Here is how SDP fits:

(1) Quantum-safe holders are not touched. Hold forever. (2) For quantum-exposed coins, the public key is on-chain. A CRQC will derive the private key. It is "exploited by adversary" or "recycled to miners." Spendability depends on cryptographic security assumptions. (3) The opt-out exists. Key rotation to a safe address. (4) Bitcoin already restricts spendability via consensus: OP_RETURN is provably unspendable, invalid scripts are unspendable, pre-SegWit anyone-can-spend outputs became restricted after activation. SDP adds one more condition, not a new category of action.

Szabo: *"The best TTP of all is one that does not exist, but the necessity for which has been eliminated by the protocol design."*[9] No committee decides what happens to these coins. The protocol does.

7.1 Consensus Change Scope

SDP modifies spend validity rules. After activation, P2PK UTXOs created before the cutoff height are no longer valid transaction inputs. This is a consensus-level change requiring broad agreement among developers, miners, node operators, and economic stakeholders. The activation timeline spans years, with BIP-9 miner signaling at a 95% threshold.

7.2 Why Not Just Freeze?

BIP-361 already solves the quantum problem. Freezing quantum-exposed coins prevents exploitation. SDP does not dispute this. BIP-361 is the minimal, conservative rule change and, given Bitcoin's deserved conservatism around consensus, it is the more likely path to activation. SDP is the more ambitious proposal: it accepts greater controversy in exchange for addressing the security budget alongside the quantum defense. SDP asks: once coins are frozen because their cryptographic protection has degraded, what should happen to the value? It can sit frozen indefinitely, contributing nothing. Or it can integrate into the block reward structure that secures every other coin on the network. Freezing solves quantum. SDP solves quantum and addresses the security budget. That additional step is the one that requires justification, and the one this proposal exists to debate.

8. Implementation

Bitcoin Core already stores creation height (nHeight) for every UTXO. Script type is deterministic from the scriptPubKey. The pieces are there. The donation pool is not a separate data structure: it is derived from the UTXO set (sum of P2PK UTXOs where nHeight < DORMANCY_CUTOFF), deterministic and reorg-safe. The spending restriction applies only after an activation height, not retroactively — same model as SegWit and Taproot deployment.

```
const DORMANCY_CUTOFF = 1035000; // ~Jan 3, 2028 (key-rotation deadline)
const DONATION_FLOOR = 100000000; // 1 BTC

// Consensus validation:
if (IsQuantumExposed(utxo.scriptPubKey)) {
  if (utxo.nHeight < DORMANCY_CUTOFF)
    return REJECT_DORMANT_QC_EXPOSED;
}
// Quantum-safe: no check. Hold forever.

// Block reward with donation halving:
const INITIAL_GAP = 21875000; // 0.21875 BTC
CAmount GetBlockReward(int height) {
  subsidy = GetBlockSubsidy(height);
  if (subsidy < DONATION_FLOOR) {
    don_halvings = (height - 1260000) / 210000;
    cap = INITIAL_GAP >> don_halvings;
    remaining = BlocksLeftInEra(height);
    available = pool_balance / remaining;
    return subsidy + min(cap, available);
  }
  return subsidy;
}
```

Table 6. Code impact by component.

Component	Complexity	~Lines
IsQuantumExposed() check	Low	50–100
Dormancy validation	Low	50–100
GetBlockReward() + donation	Moderate	200–300
Donation pool	Moderate	500–800
Coinbase donation message	Low	50–100
Wallet alerts + migration	Moderate	300–500
RPC + tests	Required	600–1,200
Total		**~1,800–3,100**

Comparable in code volume to Taproot. Simpler cryptographically — no new signature schemes. Requires a hard fork (not a soft fork like Taproot). The comparison is to implementation complexity, not deployment difficulty. A hard fork requires near-universal node upgrade.

9. Fact vs. Assumption

9.1 Verified

3–4M BTC lost (Chainalysis); 1,720,270 BTC across 45,257 P2PK UTXOs at block 892,385 (Mempool.space UTXO set report); ~1.1M BTC Satoshi (Patoshi pattern); block reward < 1 BTC at halving 6 (source code: 50*COIN >> 6); CRQC 2030–2040+ (Google roadmap ~2029, NIST deprecate ECC 2030, disallow 2035, skeptics project 2040 or later); nHeight stored in chainstate; coinbase scriptSig supports arbitrary data (BIP-34); 21M cap preserved; requires hard fork; all Satoshi quotes verified via Satoshi Nakamoto Institute; prior proposals (PoAR, #31941) criticized/rejected.

9.2 Unproven

"Only abandoned coins affected" (edge cases: imprisoned, persecuted holders). "Quantum problem solved by timing" (depends on CRQC arrival vs. trigger date). "1 BTC floor is optimal" (parameter choice, no economic modeling). "Block ~1,035,000 is the right cutoff" (governance decision — not derivable from cryptography or first principles; this is the point where SDP crosses from cryptographic mechanism into politics; the community must choose it, and that choice is inherently political). "Self-selecting mechanism" (assumes awareness). "Hard fork achievable" (Bitcoin has never executed a contentious hard fork).

This mechanism does not exist. Zero code. Zero simulation. Zero peer review. It is a concept. Evaluate accordingly.

10. Anticipated Objections

Table 7. Critics and defense.

Objection	Defense
"This is confiscation"	Ownership is not revoked. Spendability is conditional on cryptographic security assumptions. P2PK keys are exposed on-chain. If ECDSA degrades, private keys are derivable by anyone. SDP provides a multi-year key-rotation window. One transaction preserves ownership forever.
"Core design set in stone"	Satoshi changed consensus rules himself. Aug 15, 2010: block 74,638 created 184B BTC (integer overflow). Satoshi released v0.3.10 within 5 hours; chain reorganized by block 74,691. He also added 1MB limit, OP_NOP, alert system after v0.1.
"No contentious hard fork precedent"	True — biggest barrier. But the value overflow fix was a consensus-breaking change. SDP requires community consensus: "Any needed rules and incentives can be enforced with this consensus mechanism."
"Dangerous precedent"	The condition is cryptographically specific: public key on-chain or not. Binary, deterministic, verifiable by any node. Phase 1 targets P2PK only — a fixed, shrinking set. Extension to any other type requires separate technical justification and consensus.
"Holders who can't migrate"	Valid edge case. But same holders face same cryptographic degradation regardless. Their public keys are exposed. Without SDP, those keys are exploitable by any adversary with a CRQC. Pre-signed time-locked migrations and multisig estate plans can mitigate.
"21M cap is sacred"	SDP does not touch 21M cap. MAX_MONEY unchanged. Zero new coins. Security-conditional reallocation, not inflation. "Completely inflation free" (Whitepaper, Sec. 6).
"Miners shouldn't get free coins"	Miners secure every coin on the network. "The incentive may help encourage nodes to stay honest." (Whitepaper, Sec. 6). Alternative: quantum attackers get 1.72M BTC for free.
"Fees will be sufficient"	SDP doesn't contradict fee reliance — donation is supplemental and halves geometrically (5.3% of pool ever used). If fees are sufficient, donation is negligible. If not, it's a safety net.
"If Satoshi returns"	Key rotation: one transaction to a quantum-safe address. Coins preserved forever. If keys are lost, the exposed public keys face the same ECDSA degradation as any other P2PK. The opt-out is available to any keyholder.

10.1 The Value Overflow Precedent

On August 15, 2010, block 74,638 created 184,467,440,737 BTC from an integer overflow[14]. Satoshi published v0.3.10 within 5 hours. The chain reorganized by block 74,691. He did not say "the code is set in stone." He fixed it. Bitcoin's price rose 300% by year's end.

Rules can change when the threat is real. Satoshi initiated such changes himself. The market rewarded it. Different threat (quantum, not overflow). Same principle.

11. Proposed Timeline

There is no rush. The donation does not activate until the subsidy drops below 1 BTC, around 2032. That gives roughly six years to discuss, review, implement, test, and let miners decide.

Phase	Period	Description
Concept	2026	Publish the proposal. Post it to the bitcoindev mailing list and let people pick it apart. If the idea has a fatal flaw, this is where it dies.
BIP Draft	2027	If the concept survives, write a formal BIP. Independent security review of the consensus changes. Miners and pool operators weigh in on the game theory. This takes time. It should.
Code	2027–28	Open a Bitcoin Core pull request. The changes are small — a few hundred lines touching validation, reward calculation, and coinbase serialization. The test suite matters more than the implementation.
Testnet	2028–29	Run it on testnet and signet. Simulate multiple halving eras. Make sure the donation decay and pool accounting hold up. Let it run long enough that people can see it working, or see it fail.
Activation	2030–31	Miners signal support through version bits, same mechanism as SegWit. 95% threshold in a retarget period. If they signal yes, it locks in. If they don't, it doesn't. Nobody can force this.
Donation	~2032	The subsidy drops to 0.78125 BTC. The gap appears. The first donation fills it — 0.21875 BTC from the pool to the miner. Recorded in the coinbase. From here, it halves every 210,000 blocks and never stops.

Dates are approximate. Nothing moves forward without consensus. If it takes longer, it takes longer.

11.1 Deployment & Consensus Considerations

SDP requires a hard fork. Bitcoin has never executed a contentious hard fork. The value overflow fix (2010) was consensus-breaking but uncontroversial. SDP's justification is less clear-cut: reasonable people disagree on quantum timelines and fee sufficiency. For this reason, SDP requires broad agreement among developers, miners, node operators, and economic stakeholders; a long activation horizon; BIP-9 miner signaling with a 95% threshold; phased deployment (P2PK first, with separate consensus for any extension); and a community-defined expiry if the BIP does not activate within a specified number of retarget periods. If the community rejects SDP, it does not activate. This proposal is a starting point for discussion.

12. Conclusion

SDP restricts spendability of outputs whose cryptographic security assumptions have degraded. Unlike prior proposals that target all UTXOs regardless of cryptographic status, SDP applies only to P2PK addresses with exposed public keys, activates only when the security budget needs supplementation, and provides a multi-year key-rotation window. If no cryptographic break occurs, no additional value enters circulation.

The implementation is comparable to Taproot in code volume. Remaining value from restricted outputs integrates into block rewards. Quantum-safe holders are never touched. The 21M cap holds.

Satoshi described lost coins as "a donation to everyone." SDP makes that operational — spendability becomes conditional on cryptographic integrity. Ownership is not revoked. Security assumptions evolve.

> *"Any needed rules and incentives can be enforced with this consensus mechanism."*
>
> — Satoshi Nakamoto, Bitcoin Whitepaper, Conclusion

References

[1] Chainalysis, "Bitcoin's Lost Coins." Unchained Capital, "How Many Bitcoin Are Lost?" 2023.

[2] Mempool.space, "UTXO Type Distribution," block 892,385, 2026.

[3] Google Quantum AI, Willow chip (105 qubits, 2024); roadmap targets error-corrected QC ~2029. Google (2025): secp256k1 breakable with <500K physical qubits. NIST IR 8547: deprecate ECC by 2030, disallow by 2035. F. Valsorda, "A Cryptography Engineer's Perspective on Quantum Computing Timelines," 2026.

[4] S. Nakamoto, BitcoinTalk forum, February 14, 2010.

[5] PoAR, "Proof-of-Activity Reclamation," GitHub Gist, 2025. bitcoindev mailing list discussion.

[6] Bitcoin Core Issue #31941, "Proposal for Bitcoin Expiration Mechanism," GitHub, 2025.

[7] Freicoin, "Bitcoin with demurrage," freico.in, 2012.

[8] BIP-361, "Post-Quantum Migration and Legacy Signature Sunset," Lopp, Papathanasiou, Smith, Ross, Vaile, Dallaire-Demers. Assigned Feb 2026, merged Apr 2026.

[9] N. Szabo, "Trusted Third Parties Are Security Holes," 2001.

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[11] S. D. Lerner, "The Patoshi Mining Pattern," 2013–2019.

[12] Bitcoin Core source: GetBlockSubsidy(), consensus/amount.h (MAX_MONEY), struct Coin (nHeight).

[13] BIP-34, "Block v2, Height in Coinbase," 2012.

[14] Bitcoin Wiki, "Value overflow incident," block 74,638, August 15, 2010. Satoshi Nakamoto Institute, thread #186.