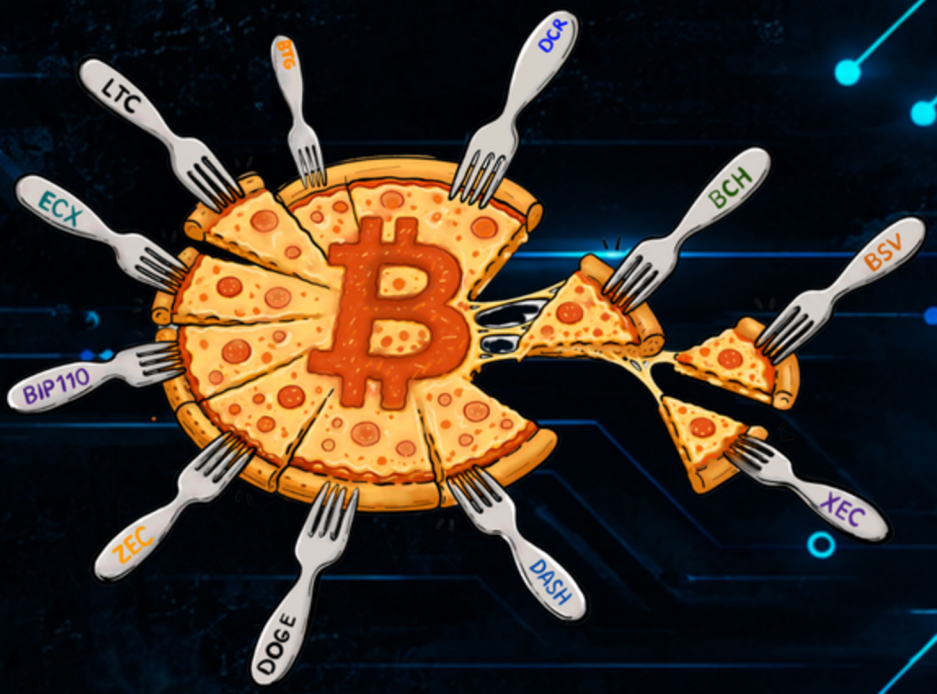
BTCTKVR
FORKS!



Ani 2026



You Can Sponsor This Magazine

BitcoinTakeover@protonmail.com

VLAD

ANI

CM



TEXT, EDITING & CONCEPT

COVERS AND ART WORKS

GRAPHICS & DESIGN

CONTENTS



BITCOIN 1



BITCOIN CASH 2



BITCOIN BLAKE2B XBT 3



ZCASH 5



ECASH ECX 4

WHAT THE FORK?!



Forks are an integral part of the Nakamoto consensus. Satoshi gave us an amazing way to solve the double spending problem and handed out the blueprint to create unstoppable internet money... but he also left us with a governance problem that still causes division and outright tribal wars between bitcoiners.

As long as everyone agrees with the ongoing network rules, there is no fork. But Bitcoin still has very limited scalability, cannot do complex contracts, and doesn't issue a fungible currency that's truly censorship resistant. There isn't even a system in place to veto the developers' technical consensus: so if the code wizards make changes that you don't like, the best you can do is operate and maintain old software that might just get deprecated or become incompatible in the future.

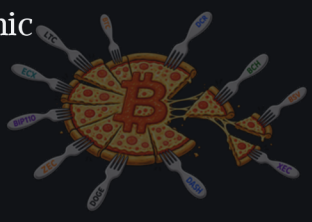
So when network participants have greater expectations from Satoshi's design, for reasons which concern network upgrades or policy changes... well, that's when the pain begins. The rebels have three choices:

1. Play the political game in order to try to convince everyone in Bitcoin to update the code;

2. Coordinate a breakaway movement which divides the network, but continues to mine blocks on a new parallel blockchain;

3. Start a new coin from the genesis block, with new rules and unique features.

If a large majority of participants agree with the change, they can leverage their power to blackmail the minority into upgrading. It's very political, except that voting, violence and first class citizenship rights are replaced by Proof of Work mining and economic incentives.

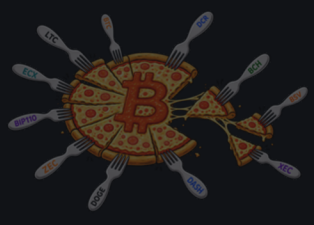


Completing the first quest requires "consensus": a situation of unanimity in which no significant participant expresses any objection. The issue is, however, that significance is very difficult to define or measure. The largest holders don't have authority because Bitcoin is not a Proof of Stake system. The miners try to avoid getting involved in politics unless they're safe from ostracization... because they are afraid of losing individual hashers, and reputation is important for their revenue. The nodes themselves don't control the network because otherwise Bitcoin would get Sybil attacked. And the developers are usually unwilling to take responsibility for any controversial proposal because it affects their ability to receive grants and any resulting bug can diminish the market valuation of the project (therefore devaluing their personal savings too).

To put it plainly, Bitcoin is stuck in a game theory that makes it safe to do nothing. If anything, arguing in favor of protocol ossification and expressing concerns about any improvement proposal on very predictable grounds (increasing complexity, unknown exploits that nobody thought about yet) is respected enough to get rewarded by conference organizers and orthodox podcasters. Yes, Bitcoin is supposed to be hard to change and that's part of the value proposition. But when the network participants can't even agree on the necessity to deploy upgrades and there's a fairly large faction that argues in favor of stagnation, that's where the forking becomes legitimate.

But this game gets even more complicated once you realize that in Bitcoin, unlike traditional political systems, nobody wants to have an evident majority. Controlling a large share of the mining hash rate, routing a significant chunk of the economic activity, and even hiring too many developers can be perceived as a sign of centralization. This centralization relies on trusted third parties and single points of failure... and the consequence is that the project at large gets perceived as being less valuable because it's not sufficiently decentralized. If anyone takes too much action, it's possible that the price of bitcoin will actually go down. So the question is: what is the right amount of action? Where do we strike a balance?

Bitcoin is the only political system in the world where nobody wants to form a majority, nobody wants to appear that they're in charge, and nobody wants to be held accountable. It's a weird and counterintuitive system whose resilience to change can also get exploited by its enemies: if this unprecedented form of internet money never becomes a threat to the mainstream financial system and actually gets coopted by those who would normally be obsoleted by such an innovative network, then nothing ever changes and all the libertarian dreams fade. Printing money is cheap. Allocating a small amount of this money to keep Bitcoin under control is a trivial expense in the grand scheme. And for better and for worse, "number go up" is the ultimate form of consensus... as everyone agrees that it's good for the project and nobody will dare to fight against it.



But as we've seen over the last decade, price increases do not guarantee that any meaningful development will happen. Bull markets do bring in more smart people, more developers willing to put their time and effort into making the project successful, and more academics who do research that pushes the limits of Satoshi's design. Some of the best ideas receive funding and get deployed on test networks. Some of the brightest Bitcoin developers travel the world to explain their ideas on conference stages. The problem is that eternal "bikeshedding" and a predictable repetition of the same critical concerns result in no meaningful progress.

So once the improvement proposal never gets merged into the code due to lack of consensus, what should the developers do? Should they set years of their work on fire, never to attempt to test it on a financial network with real incentives? Should they accept defeat and move on to other things? Or perhaps they can prove the merits of their idea, while also collecting precious market information about the actual value of this upgrade. This is when forking becomes imperative.

Sure, most altcoins are doomed to fail. Historically, the Bitcoin hard forks haven't been able to capture the same market valuation or network effect either. But in this world of free markets and free open source software, why not give it a try? Worst case scenario, the critics were right and the entire initiative was a mistake. But if it works out, Bitcoin can finally have a worthy competitor.

In an ideal scenario, everyone is on board with every meaningful upgrade. But in a decentralized network, it's very difficult to reach consensus. As a matter of fact, the term "consensus" is often cited in order to stall progress, or else effectively kill off an improvement initiative. There's "technical consensus" which stalled OP_CTV according to Dr. Adam Back. There's social consensus which never allowed BIP101 and its sibling block increase proposals to get activated. There's "rough consensus" which is being used against OP_CAT and other attempts to restore Satoshi's old disabled OP codes.

Faced with this reality, where the developers who maintain the Bitcoin project will only accept a utopian unanimity that any malevolent actor can break, we end up having forks: versions of Bitcoin that follow pretty much the same rules, try to reach the same goal, share most of the original codebase, but seek to accomplish the mission in a different way or through different technical or political means. Which is really beautiful for computer science nerds who are accustomed to the Linux model where every minor disagreement leads to the creation of a new distribution. But for economists, it's a confusing situation where competing currencies that are 90% identical are going through a multi-year price discovery phase in order to gain network effects and figure out the value of new ideas. Maybe one day one such fork will dethrone the original Bitcoin due to ingenuity of design and large-scale adoption on markets. Or maybe we will be stuck in this pet rock phase forever, making bets against inflating fiat currencies without ever replacing them.



While Satoshi Nakamoto was around, the world knew nothing but Bitcoin. But as soon as he left the project in the hands of the Core development team, political struggles emerged. And for every rejected proposal, we had a bunch of developers launching a new cryptocurrency network to experiment with the unpopular features. Many of these projects died over the years... yet today we still have a handful of them that survived and were able to find their own market and use cases.

From a rather practical and cynical perspective, one can argue that Bitcoin scales and adds new features through forks. So everything that builds on the same original codebase is a Bitcoin, the only inconvenience is that there are multiple currencies with different security models that are priced by the market individually according to their merits. If BTC doesn't scale and doesn't have privacy, one can use Zcash. If the fees are too high on the original chain, BCH and Litecoin come to the rescue. And if this whole movement appears to be too serious, with institutions and high-profile politicians getting involved, it can also become appealing to people looking to have some fun via Dogecoin.

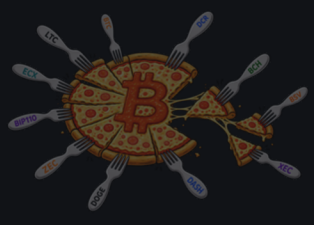
The market provides options for everyone... but fundamentally, the technology is still Bitcoin. This is a hard pill to swallow for maximalists and a complex problem to solve by economists and game theoreticians. But the reality is that forks really do extend Bitcoin: they add capacity and features, but print money too. Yet is it really so terrible if we replace the hundreds of political central bank-controlled fiat currencies with a dozen blockchains that provide utility to billions of users via cryptocurrencies that can be swapped at the global market rate? 1 billion censorship resistant coins with predictable monetary policy are definitely better than infinite numbers in Excel spreadsheets that the government can control. I like to call this way of thinking Bitcoin post-maximalism... but I guess that's a subject for another magazine!

This magazine explores three types of forks:

1. The hard forks and soft forks that improved the original Bitcoin chain;

2. The breakaway hard forks, which copied the UTXO set (coin ownership) but moved it to a new network with new rules and features: Bitcoin Cash, Bitcoin SV, Bitcoin Gold, Amaury Sechet's eCash (XEC), Luke Dashjr's Blake2b XBT, and Paul Sztorc's BIP300 eCash (ECX);

3. The codebase forks, which took Satoshi Nakamoto's code and tried something new by starting a new blockchain from scratch (Namecoin, Litecoin, Dogecoin, Dash, Decred, Zcash);

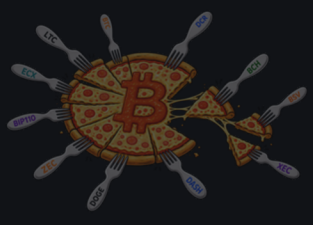


In order to make this publication unique, I used quotes from interviews with founders and developers which I have interviewed over the years on Bitcoin Takeover Podcast. Even though you can find the data about every fork elsewhere, it's the personal input and commentary of the people involved that makes this effort truly one of a kind.
This magazine was designed in September 2026, with a first digital demo to be presented at Token2049 in Singapore (October 7–8) and a first demo print consisting of 5 articles to be launched at Tabconf 8 in Atlanta, USA (October 12–15). The final version, featuring all 13 articles and some bonuses, will be presented at the Bitcoin Conference in Amsterdam (November 5–6). All contents can be found on the bitcoin-takeover.com page, so anyone can access the information for free.

But the information without gorgeous eye-catching graphics can be boring. So I would like to thank Ani for doing the stunning watercolor painting for the cover and the clean graphics for the BTC article (with more work on the way). I also want to thank CM for jumping in to help: his work ethic is amazing, his comic book-style graphics are jaw-dropping, and without his "one article per day" routine the demo wouldn't have been ready on time. So kudos to both of them for turning my text into something that's visually pleasing.

I would also like to thank my podcast sponsors Cake Wallet, LayerTwo Labs, Sideshift.ai, Orange Rock, and Braiins Hashpower for supporting my work over the years. It's thanks to them that nice projects like this magazine can see the light of day (just like Vaultoro, Wasabi and Trezor made the first BTCTKVR magazine happen in 2021). Yes, HODLing is nice. But creating beautiful art is what gives life meaning and how others will remember us.

So is Bitcoin a monolithic project or a codebase? Did Satoshi Nakamoto give us the blueprint to create unstoppable internet currencies, or did he bring into existence the final form of money and the only one we will ever need? Is there any value in trying these forks? There is only one way to find out: through study, free markets and research, not dogma.





Bitcoin The Orginal chain, slightly upgraded

EveryconsensusupgradeBitcoinhas ever switched on without splitting its ledger

While most of the forks featured in this magazine were born the moment a group of people decided they could no longer share a blockchain with everyone else, this particular article is about the opposite behavior. It's about the times Bitcoin changed the rules and everybody stayed. Eight times since 2012, the network has tightened what counts as a valid block. Eight times the chain, the coins, and the history carried on as one. Here is a comprehensive list that describes how each change was switched on, and the handful of cases where the story is messier than the block height suggests.

Soft forks tighten the rules, hard forks change them

What's in scope for this particular article is soft forks and genuine, general will hard forks that changed the consensus rules of Bitcoin mainnet while keeping one continuous chain and one continuous set of unspent coins.
For now, we won't cover the coins that split off with their own copy of the ledger (Bitcoin Cash, Bitcoin SV, Paul's eCash BIP300 fork and friends). We will also not take into account peer-to-peer changes that never touched block validity (BIP37 bloom filters, for example), address formats that only encode rules already in force, and relay policy that a node applies to its own mempool but not to blocks.
For the sake of correctness, it's worth noting that research stopped on September 17th 2026. Heights follow the mainnet parameters shipped in Bitcoin. Core's src/kernel/chainparams.cpp, or the BIP text where Core still runs the deployment through version bits (Taproot).

Activation times are the header time field of the activating block, read from mempool.space and shown in UTC, unless a BIP fixed a flag-day timestamp instead.

Two caveats worth knowing: a block's header time is set by the miner and can drift a couple of hours from wall-clock time, and Core has quietly rewritten several old activations into simpler height checks (BIP90). So the code you read today is not always the code that ran at the time. Maybe there's a reason why Satoshi decided to not name it the "timechain" (as the pre-release version of Bitcoin called it in November 2008) and opted for blockchain instead. Probably the best reason would be that Bitcoin is bad at telling the time, even if some people use block height for time stamping events.

Has Bitcoin ever hard forked?

No intended hard-fork upgrade has ever activated on the Bitcoin chain. The project's tradition is to tighten rules rather than loosen them, so that a node running old software still follows the majority chain even if it cannot fully validate the new features. The one serious attempt at a coordinated hard fork of the main chain, the SegWit2x block size increase proposed in the 2017 New York Agreement, was called off before its planned block 494,784 activation. BIP101, 102, 103, and every other proposal to increase the block size has only been debated, without benefiting from a clear activation path.

But the honest answer is that Bitcoin's chain has split by accident twice in its existence, and one of the incidents is arguably a hard fork.

First there's the 2010 value overflow. On August 15th 2010, at block height 74,638, a transaction created roughly 184 billion bitcoin through an integer overflow. Satoshi Nakamoto quickly patched the software to launch version 0.3.10. The new client added the missing range check, miners reorganized the chain about 53 blocks later, and the bad block vanished from history. The inflation bug fix was a tightening, so it counts as a soft fork with an unusually violent activation.



Then there’s the March 2013 database split Bitcoin 0.8 replaced Berkeley DB with LevelDB and, without anyone realizing, removed an implicit limit of about 10,000 database locks that older versions hit when processing large blocks. On March 11th 2013,block 225,430 triggered a split of at least 24 blocks.To end this accidental fork, the pools downgraded their software to version 0.7. During the confusion that ensued, one experimental double spend succeeded. Version 0.8.1 shipped a temporary rule (no more than 4,500 transaction IDs referenced by inputs in a block) that expired on May 15th 2013 .

On August 16th 2013, block 252,451 finally exceeded the old limit and forked unpatched nodes off for good. BIP50, the post-mortem, later removed the words "hard fork" because the limit was never a written rule and varied from node to node. BitMEX Research and Jameson Lopp both argue that, on balance, it was one anyway. To please every side of the debate, let’s say that this was the closest Bitcoin has come to hard forking.

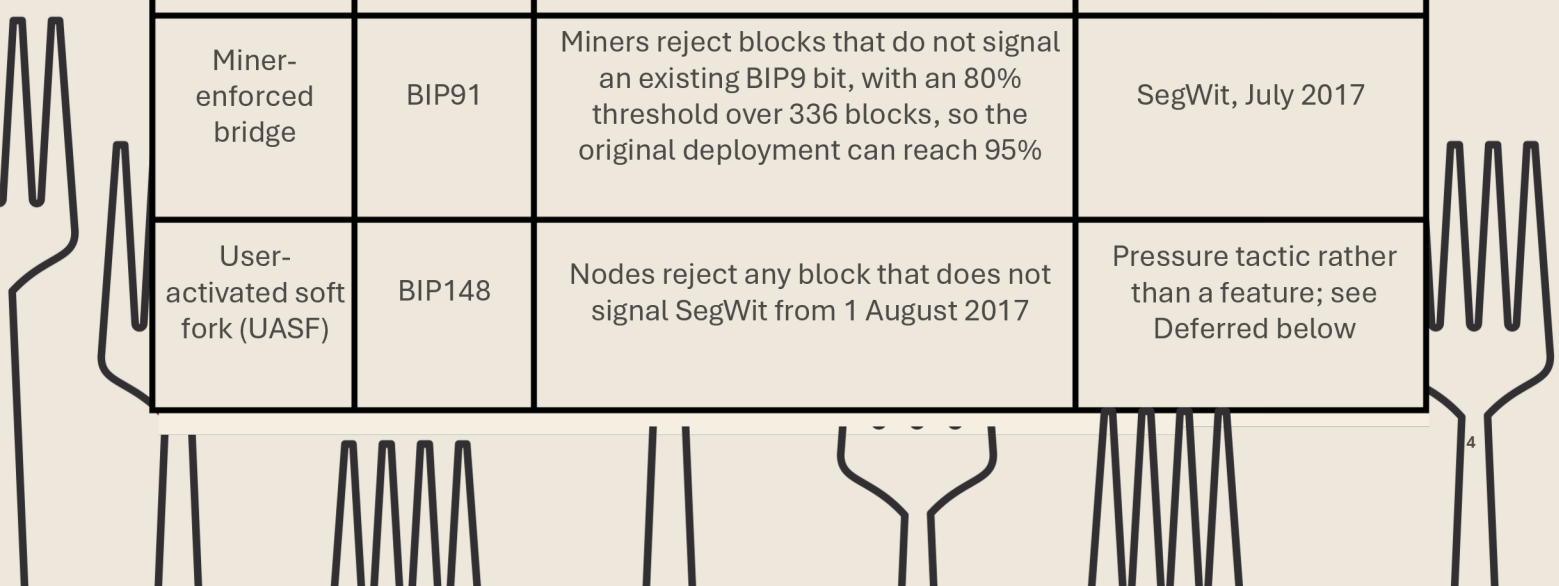
A third, quieter case was CVE-2018-17144. Disclosed in September 2018 by a Bitcoin Cash developer, this bug would have let a miner spend the same input twice within a block. Core versions 0.14.0 to 0.16.2 carried it. No block ever exploited it, so no split occurred… but strictly speaking, those versions had loosened a rule without anyone noticing and the patch tightened it back. If the entire network updates to the latest version of the client in order to make a change, is that not a hard fork? Well, you could argue that the older broken version is still in consensus and therefore anyone can run it. But in practice, it’s unsafe to do so and every network participant chooses to make the switch.

How a soft fork gets switched on

Bitcoin has never had one fixed procedure for soft fork activation. Each generation of developers attempted to fix the failures of the previous one. As you can see in the table below, there are seven different ways… and every time a new proposal emerges (such as BIP300, CTV, or OP_CAT), the community must figure out how to reach the fabled consensus.



MECHANISM	DEFINED IN	HOW IT WORKS	WHERE IT WAS USED, AND WHAT WENT WRONG
Flag day after a miner poll	BIP16 pattern	Miners put a marker (/P2SH/) in coinbase text; if support looked sufficient, enforcement began at a fixed timestamp	P2SH, 2012. Fragile: the date slipped twice (1 Feb, 1 Mar, then 1 Apr) and an early enforcement bug produced the block 170060 exception
IsSuperMajority (ISM)	BIP34 pattern	Nodes count block nVersion over the last 1,000 blocks: at 750 the new rule is enforced on new-version blocks, at 950 old-version blocks are rejected	BIP34, BIP66, BIP65. No timeout, and only one upgrade could run at a time
Version bits	BIP9	Each proposal gets its own bit in nVersion, a start time and a timeout (both median-time-past); 1,916 of 2,016 blocks (95%) in one retarget period locks it in, and it activates one period later	CSV suite (bit 0), SegWit (bit 1). Gave miners an effective veto, which the SegWit fight exposed
Version bits with forced lock-in	BIP8	BIP9 measured in heights instead of time, with an optional lockinontimeout that makes signaling mandatory in the final period	Debated at length for Taproot; never used for a mainnet activation. BIP343 was a parallel BIP8 (LOT=true) client that stayed compatible with Speedy Trial
Speedy Trial	BIP9 variant, described in BIP341	Short signaling window (about three months), 1,815 of 2,016 blocks (90%), plus a min_activation_height that delays enforcement	Taproot, 2021. Locked in within seven weeks
Miner-enforced bridge	BIP91	Miners reject blocks that do not signal an existing BIP9 bit, with an 80% threshold over 336 blocks, so the original deployment can reach 95%	SegWit, July 2017
User-activated soft fork (UASF)	BIP148	Nodes reject any block that does not signal SegWit from 1 August 2017	Pressure tactic rather than a feature; see Deferred below



BEFORE THERE WERE BIPs

Thelist below starts in 2012 because that is when Bitcoin began announcing rule changes in advance. Satoshi tightened the rules several times in 2010 with nothing more than a software release, so these have version numbers rather than clean activation heights. BitMEX's fork history warns that no precise date can be given where the change went through without a split.

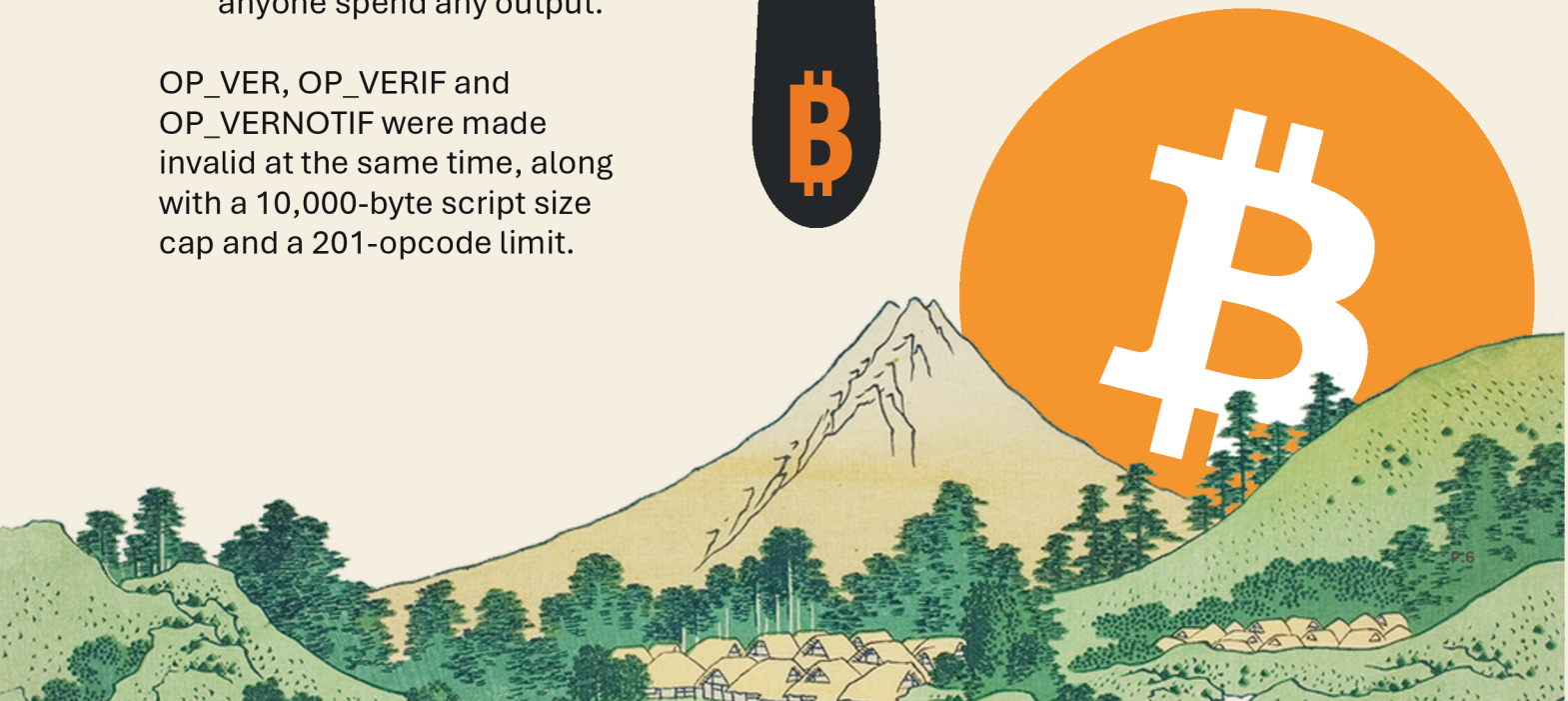


- July to August 2010 (0.3.5 to 0.3.8): a batch of script opcodes was disabled outright, among them OP_CAT, OP_SUBSTR, OP_LEFT, OP_RIGHT, OP_INVERT, OP_AND, OP_OR, OP_XOR, OP_2MUL, OP_2DIV, OP_MUL, OP_DIV, OP_MOD, OP_LSHIFT and OP_RSHIFT, after a bug let anyone spend any output.

OP_VER, OP_VERIF and OP_VERNOTIF were made invalid at the same time, along with a 10,000-byte script size cap and a 201-opcode limit.

- August 2010 (0.3.10): output value range checks, the response to the overflow described above.
- September 2010 (0.3.12): the 1,000,000-byte block size limit and the 20,000 signature-operations limit, written into the code so that enforcement began at block 79,400.

None of these was announced as a fork. All of them still bind every block mined today.





The eight activated soft forks

These Bitcoinupgradesareorderedbytheblockheightatwhichthey were activated."Core"isthefirstreleasethatshippedtherule.

#	UPGRADE	BIPS	HEIGHT	ACTIVATION (UTC)	METHOD	CORE
1	Pay to Script Hash (P2SH)	BIP16	173,805 (first block after the flag day)	Flag day 2012-04-01 00:00; block 173,805 mined around 00:43	Flag day after /P2SH/ poll	0.6.0
2	No duplicate transaction IDs	BIP30	Timestamp rule at first, later applied to every block except 91,842 and 91,880	2012-03-15 00:00 (blocks with header time above 1331769600)	Flag day, later extended	0.6.0 era
3	Block height in coinbase	BIP34	227,931	2013-03-25 07:30:09	ISM on version 2	0.7.0
4	Strict DER signatures	BIP66	363,725	2015-07-04 01:54:32	ISM on version 3	0.10.0
5	CHECKLOCK TIMEVERIFY (CLTV)	BIP65	388,381	2015-12-14 17:24:44	ISM on version 4	0.11.2
6	CSV suite (relative locktime)	BIP68, BIP112, BIP113	419,328 (locked in from 417,312)	2016-07-04 23:16:01	BIP9 bit 0, "csv"	0.12.1
7	Segregated Witness (with NULLDUMMY)	BIP141, BIP143, BIP147 (BIP144 for P2P)	481,824 (locked in from 479,808)	Lock-in 2017-08-09; active 2017-08-24 01:57:37	BIP9 bit 1, pushed over the line by BIP91 and BIP148	0.13.1
8	Taproot	BIP340, BIP341, BIP342	709,632 (locked in at block 687,285 on 2021-06-12)	2021-11-14 05:15:27	Speedy Trial, bit 2, 90%, minimum activation height	0.21.1

What each one actually did?

in a sentence: P2SH let a sender pay to the hash of a script so the recipient carries the complexity (the origin of addresses starting with 3). BIP30 closed a loophole in which two transactions could share an ID. BIP34 forced miners to write the block height into the coinbase, which made BIP30's problem impossible in practice. BIP66 stopped relying on OpenSSL's forgiving signature parser, after it turned out that different parsers could disagree on validity. CLTV gave Bitcoin its first absolute timelock opcode. The CSV suite added relative timelocks (BIP68 in the sequence field, BIP112 as an opcode) and made a block's locktime comparisons use median-time-past (BIP113), the plumbing that Lightning channels depend on. SegWit moved signatures out of the transaction ID, fixing third-party malleability and raising capacity through the weight limit, while NULLDUMMY removed a small malleability vector in multisig. Taproot introduced Schnorr signatures, a new output type where a single key and a tree of scripts look identical on chain, and a cleaner script version for the future.

The BIP's results section records the last version-1 block as 227,835. Core's BIP34Height is 227,931 (hash ending 080b8b), the point at which its simplified BIP90 check begins. Use 227,931 as the enforced activation height and cite the BIP text for the last-v1 story.

SegWit: lock-in versus activation. The BIP9 state machine reached LOCKED_IN at height 479,808 (August 9th 2017) and ACTIVE one retarget period later at 481,824 (August 24th 2017). Both dates circulate as "the SegWit date"; only the second is when the rules took effect.

BIP30's two exceptions. Blocks 91,842 and 91,880 contain coinbase transactions that duplicate those of blocks 91,812 and 91,722 respectively. They are grandfathered forever. Core also stops checking BIP30 once BIP34 is active, except that it must resume at height 1,983,702, where a version-1 block's coinbase could collide with a BIP34-style serialized height.

Where the block heights are contested?

BIP34: 227,835 or 227,931?

BIP91: a mechanism, not a feature

BIP91 ("Reduced thresholdSegwit MASF") added no script rule of its own. From late July 2017 miners running it rejected blocks that did not signal SegWit's bit 1, which pushed the original BIP9 deployment past 95% and averted the 1 August UASF deadline. It belongsin theSegWit factsheet under activation politics; a standalone sheet is optional.

Deferred: proposals that shaped the story without becoming rules

These are tagged "deferred, scope expansion" and must not be counted as activated upgrades.

ITEM	WHAT IT WAS	WHY IT SITS HERE
BIP148 UASF	Nodes reject non-signaling blocks from August 1st 2017	An activation tactic and a coordination story, not a new script feature
SegWit2x (NYA, btc1 client)	A 2 MB base block hard fork planned for block 494,784, roughly three months after SegWit	Suspended on November 8th 2017; would have hard forked BTC; the politics fed the Bitcoin Cash split at block 478,559 on August 1st 2017
BIP149	A second SegWit deployment using BIP8 with a 2018 forced timeout	Made unnecessary once BIP91 and BIP148 forced the issue
BIP62	Cer A catalogue of malleability fixes	Withdrawn as written; its parts resurfaced as BIP66, NULLDUMMY and SegWit
OP_EVAL (BIP12)	Gavin Andresen's first attempt at pay-to-script	Rejected for allowing unbounded recursion; replaced by BIP16 (and BIP17, another alternative, also lost)
Covenant and other future proposals	OP_CTV (BIP119), OP_CAT revival (BIP347), LNHANCE and others	Not activated as of the research date; out of scope until one is

Explicitly out of scope

- BIP37 bloom filters: a peer-to-peer privacy and denial-of-service topic, not consensus.
- BIP70 payment protocol: application layer.
- Address encodings BIP13, BIP173 (bech32) and BIP350 (bech32m): they describe how to write down outputs whose rules P2SH, SegWit and Taproot already define.
- Relay and standardness policy changes that never applied to block validity.



BITCOIN CASH
THE BIG BLOCK BREAKAWAY

How the block size war produced Bitcoin's first durable chain split, and what nine years of bigger blocks have and have not proved

Every fork in this magazine is built on pain, frustration, anger, and ambitious of achieving something bigger than BTC. Bitcoin Cash has the most famous story arc... and possibly the most fascinating one thanks to the deep lore and years of infighting.

For roughly two years, from 2015 to the summer of 2017, the Bitcoin world argued about a single constant in the code: the one megabyte block size limit that Satoshi slipped into version 0.3.12 in September 2010 without announcing it. One camp wanted the number raised so that Bitcoin could stay cheap to use on chain. The other wanted it left alone and the extra capacity found elsewhere, first through Segregated Witness and then through second layers like Lightning. Neither side could remove the other from the network, so on the 1st of August 2017 one of them left.

I was confused at the time. I landed on BTC like most people, because if you held bitcoin you got both coins and the BTC ticker felt like the safer bet. What I disliked about Bitcoin Cash was the campaign to call itself the real Bitcoin, the way Bitcoin.com quietly became a BCH website and r/btc a BCH forum. It felt like a nasty divorce where both parties grab whatever they can carry and claim they are in the right. Nine years later I sat down with the phenomenal big blockers who stayed after the famous names left, for eight hours and fourteen minutes, and this article is the factsheet I wish I had read before that conversation... but with some elements that I could only learn after having interviewed the "bcashers".

VITAL STATISTICS



CATEGORY

UTXO hard fork: a new chain that inherits Bitcoin's entire history up to the split

SPLIT DATE

1 August 2017, by flag day (median time past 1501590000, 12:20 UTC)

LAST COMMON BLOCK

478,558, header time 13:16:14 UTC, mined by BTC.com with a /NYA/ tag in the coinbase

FIRST BCH-ONLY BLOCK

478,559, mined by ViaBTC roughly six hours later, about 1.9 MB in size

PROOF OF WORK

SHA-256d, same as Bitcoin, so the same machines can mine either chain

CHILDREN

Bitcoin SV (split 15 November 2018) and Bitcoin ABC, later eCash / XEC (split 15 November 2020). Both get their own articles.

MARKET CAP

About $4.44 billion, roughly 0.29% of Bitcoin's $1.53 trillion; CoinGecko rank 23. Peaked at rank 2 in 2017, fell to 35 in December 2018, briefly re-entered the top 10 in early 2026

PRICE

About $221; all-time high about $3786 on 19 or 20 December 2017 depending on the exchange feed; all-time low about $75 on 15 December 2018

MINING SECURITY

Difficulty about 0.33% of Bitcoin's on the same date; Coin Dance showed BTC 4.4% more profitable to mine when I checked (it had said 16% the day before, so this swings hourly)

Market figures are a snapshot from 17 September 2026 and will be stale by the time this is printed. Treat them as a scale reference, not a quote.

WHY IT SPLIT: THE POLITICS

SHORT VERSION

Bitcoin's social layer failed to reach consensus, so the code did it instead.

LONG VERSION

Starts with the whitepaper's subtitle, "**A Peer-to-Peer Electronic Cash System**." The large block camp read those words literally: if fees rise to the point where a coffee costs more to send than to drink, Bitcoin has stopped being cash. Their proposals came in waves. Bitcoin XT (BIP101, Gavin Andresen and Mike Hearn) wanted 8 MB blocks doubling every two years until 2036. Bitcoin Classic settled for 2 MB. Bitcoin Unlimited abandoned fixed numbers altogether in favor of "emergent consensus," where miners pick their own limits and the market sorts it out. None of them reached activation on the main chain.





Calin Culianu, who was there on fork day and now maintains the node software most of the network runs, told me that the forking conversations had been going on since 2015, "the same way frustrated BTC developers talk about forks today." Asked why BCH did not simply adopt Gavin's BIP101 schedule, he gave the most honest answer I have heard on the subject: "Any group of rebels is going to be reacting to the thing they rebelled against. You try to meet them halfway." The big blockers spent two years proposing compromises to plug holes that Core kept finding in their arguments, and the coin they eventually launched carried the scars of that negotiation rather than the purity of the original idea.

The small block camp saw something different in those proposals: a precedent for miners and businesses changing the money's rules by agreement among themselves, which they regarded as the worst possible governance model for a system meant to resist exactly that. SegWit, a soft fork that raised capacity by moving signatures out of the base block, was their answer. Large block advocates called it an accounting trick that handed the roadmap to Core developers and made second layer networks the only path forward.



3 EVENTS IN 2017 TURNED A DEBATE INTO A DEADLINE:

The New York Agreement (May 2017)

Digital Currency Group convened miners and businesses representing, by their count, over 80% of hashrate. The deal, branded SegWit2x, promised SegWit first and a 2 MB base block hard fork three months later. Many large block advocates distrusted it from the start; small block developers refused to sign at all. The 2x half was suspended on 8 November 2017 and never happened. It is often conflated with Bitcoin Cash, wrongly: BCH launched in August as a hedge against exactly this outcome, and only after SegWit2x collapsed did the NYA's big block constituency migrate to it.

BIP148 (The user-activated soft fork)

Node operators pledged to reject any block that did not signal SegWit from 1 August 2017. Whether or not it had the economic weight to succeed, it made 1 August the day everyone was planning around.

The UAHF (Bitcoin ABC, led by Amaury Séchet)

Published a user-activated hard fork specification in June 2017 as a counter to BIP148: if the UASF chain would reject non-signaling blocks, the UAHF chain would reject SegWit and raise the block size instead. What began as a contingency plan turned into a launch. Culianu recalls that the project briefly had no name at all ("Bitcoin user activated hard fork" was the placeholder) before Bitcoin Cash crystallized in July, in direct reaction to the UASF branding. ViaBTC listed futures before the split, and the ticker moved from BCC to BCH once it became obvious that BCC already belonged to a Ponzi scheme.

WHAT CHANGED AT THE FORK: THE TECHNICAL DELTA

Four rules separated block 478,559 from anything Bitcoin would accept, and they were designed so the two chains could never be reunited by accident

1 NO SEGWIT

Not a missing feature but a statement of intent: capacity would come from the base block, not from a witness discount.

2 REPLAY PROTECTION

Every BCH signature must use SIGHASH_FORKID, with a signature hash adapted from BIP143. A transaction signed for one chain is invalid on the other, so a coin spent on BCH stays put on BTC and vice versa. Ethereum Classic had skipped this a year earlier and paid for it. Bitcoin Cash did not.

3 THE EMERGENCY DIFFICULTY ADJUSTMENT

If fewer than six blocks appeared in twelve hours, difficulty dropped by 20%. This kept the minority chain alive when miners left for BTC, but it also created a lucrative oscillation: miners piled in when difficulty was low, mined a burst of fast blocks, then left when it rose. The side effect is still visible: BCH is 1,490 blocks ahead of Bitcoin as I write, which is why its halvings arrive weeks before Bitcoin's.

4 BIGGER BLOCKS BY CONSENSUS

The fork block had to be larger than 1 MB, which is why the first BCH block was deliberately padded to about 1.9 MB. Nodes had to start with an "excessive block" limit of at least 8 MB.

THE ROADMAP SINCE

Bitcoin Cash upgrades by scheduled hard fork, historically twice a year and since 2021 every 15 May. Every one of these would be impossible on Bitcoin without a chain split. That is precisely the point. Since the CHIP process (Cash Improvement Proposals) was introduced in 2020, fifteen CHIPs have been implemented.

DATE	CHANGE	BITCOIN, FOR CONTRAST
13 Nov 2017	EDA replaced by a new Difficulty Adjustment Algorithm (rolling 144-block window)	Kept the 2016-block retarget it has had since 2009
15 May 2018	Block limit raised to 32 MB; several Satoshi-era opcodes re-enabled (OP_CAT, OP_SPLIT, OP_AND, OP_OR, OP_XOR, OP_DIV, OP_MOD, OP_NUM2BIN, OP_BIN2NUM); OP_RETURN data raised to 220 bytes	1 MB base plus 4 million weight units; OP_CAT still disabled, revival proposed as BIP347
15 May 2018	Canonical Transaction Ordering (CTOR); OP_CHECKDATASIG; minimum transaction size of 100 bytes. The nChain camp rejected this upgrade and became Bitcoin SV	Transactions stay in topological order
15 May 2019	Schnorr signatures for CHECKSIG and CHECKDATASIG; a rule allowing coins accidentally sent to SegWit-style addresses to be recovered	Schnorr arrived in November 2021, inside Taproot only
15 Nov 2019	Schnorr for CHECKMULTISIG; MINIMALDATA enforced in consensus	No equivalent
15 May 2020	SigChecks (a new limit on signature operations per block); OP_REVERSEBYTES	No equivalent
15 Nov 2020	ASERT difficulty algorithm (aserti3-2d), designed by Jonathan Toomim. Bitcoin ABC's Infrastructure Funding Plan was rejected by the majority and ABC's chain became BCHA, later eCash	No equivalent
15 May 2021	Unconfirmed transaction chain limit removed; multiple OP_RETURN outputs allowed	Core relaxed its own chain limit only as policy
15 May 2022	64-bit script integers; native introspection opcodes that let a script inspect the transaction spending it	Covenant proposals such as OP_CTV remain unactivated
15 May 2023	CashTokens: fungible and non-fungible tokens as consensus primitives; P2SH32 (32-byte script hashes)	metaprotocols (Ordinals, Runes, Taproot Assets) on top of consensus
15 May 2024	ABLA, the Adaptive Blocksize Limit Algorithm: the limit grows with sustained demand, with a 32 MB floor	No adaptive block size, and no proposal for one under serious discussion
15 May 2025	Virtual machine limits rewritten (CHIP-2021-05) and arbitrary-precision integers in script (CHIP-2024-07 BigInt)	No equivalent
15 May 2026	Loops and reusable functions in the script VM. Developers now describe the BCH VM as explicitly Turing complete. A one-minute block time is under discussion for a future upgrade	No equivalent

A NECESSARY CLARIFICATION ABOUT SCHNORR

Bitcoin Cash shipped Schnorr signatures two and a half years before Bitcoin did, and its advocates like to point this out. Fair enough. But BCH Schnorr is a drop-in replacement inside the existing CHECKSIG opcode. Bitcoin's Taproot is a new output type in which a single key and an entire tree of alternative scripts are indistinguishable on chain until spent. They share a signature algorithm and almost nothing else. Likewise CashTokens and Ordinals are not two answers to the same question: one is enforced by every node, the other is a convention that nodes ignore.

A NECESSARY CLARIFICATION ABOUT OP_CAT

People in BTC still say with a straight face that Satoshi was right to disable it and that it would destroy the chain. Culianu's account of why it was disabled is worth recording: "Satoshi was balancing twenty plates at once. Some things he just got rid of because he couldn't deal with the consequences of a cat bomb." A script that doubled a string repeatedly could exhaust a node's memory, and in 2010 the quickest fix was to remove the opcode. BCH's answer since 2025 is to price every VM operation and cap the total per input, so no single opcode can blow up a node regardless of what it does. Robin Linus, the creator of BitVM, messaged me during the live stream: "Tell the BCH guys that I, the officially crowned king of Bitcoin script wizards, am jealous of all their neat opcodes and wish we had them too." He used a stronger adverb.



HOW BITCOIN CASH DIFFERS FROM BITCOIN TODAY

ON CONSENSUS

The two chains share every block up to 478,558 and nothing after. BCH has forkid signatures, canonical ordering, adaptive blocks, native tokens, introspection opcodes, unbounded integers and loops. It has no SegWit, no Taproot, no bech32 addresses (it uses its own CashAddr format, introduced in January 2018, precisely to stop people sending coins to the wrong chain). It also has no Replace-by-Fee. BCH removed RBF at the first opportunity and added double-spend proofs instead, because zero-confirmation acceptance at the point of sale is treated as a feature to protect rather than a risk to eliminate.

ON SCALING PHILOSOPHY

Bitcoin Cash bets that on-chain capacity should always exceed demand so that fees stay near zero and the fee market never really forms. Bitcoin bets that scarce block space and a fee market are what pay for security once the subsidy runs out, and pushes small payments to Lightning and other layers. Coin Dance's number on the day I checked was that a Bitcoin transaction cost about 359 times more in dollar terms than a BCH one. The number is real. So is the counter-argument that a chain nobody needs to pay to use is a chain nobody is paying to secure. Culianu's reply to that, for the record: with enough volume, "the price could drop 99% and the miners would still be totally secure." With current volume, that sentence is a hypothesis.

Why 32 megabytes and not BSV's gigabytes? "It's like a sweet spot number," Culianu said. "Decent block propagation, validation time, acceptable orphan rate. An engineering question." ABLA exists so that the number never has to be a political question again: the limit is now a consensus rule that follows demand, which is, as one of the developers put it, the block size wars made impossible to repeat.



ON SECURITY

Because the proof of work is identical, BCH's security budget is a function of its price. At roughly 0.3% of Bitcoin's difficulty, the cost of renting enough SHA-256 hashrate to attack it is a rounding error for a large pool. On 15 May 2026, the day of the network upgrade and with most of the developer community gathered in Ljubljana, somebody tested that. Bitcoin Core had disclosed a long-standing crash bug on 5 May; an attacker mined two deliberately malformed blocks against BCH within thirty minutes, spending an estimated 3,000 to 10,000 USD in hashrate on the assumption that the fork had inherited the bug. It had not. BCHN had removed the offending line years earlier as a code smell. The blocks were rejected as invalid, the network noticed nothing, and BCH crashed about 25% over the following days on a wall of short positions that may or may not have been related. It is the first documented hostile attack on the chain itself, as opposed to a split from within.

ON DECENTRALIZATION

Bitcoin Cash's supporters point to multiple independent node implementations (Bitcoin Cash Node, BCHD, Knuth, Verde, Bitcoin Unlimited historically) and argue that no single team controls the protocol. Critics reply that 32 MB blocks, let alone ABLA's headroom, would price hobbyist nodes out if the chain ever filled them. The BCH answer to "can you people even run nodes?" (a question I once watched a maximalist ask two BCH visitors at a conference in Frankfurt) is that the premise is wrong: SPV was in the whitepaper, UTXO commitments are on the roadmap, and Bitcoin Core itself skips signature checks on historical blocks through assumevalid. Two years ago I synced a Bitcoin Core node in 7 hours 40 minutes and a BCH node in 2 hours 20 minutes on the same MacBook Pro. The BCH chain is currently the smaller one, because it has had less traffic. Both facts cut like a twofold blade that nourishes irrational tribalism.

ON ADOPTION

BCH has stayed listed on every major exchange since 2017 and survived two hostile splits with its ticker intact. Real spending pockets exist: Townsville in Australia, Argentina, and the Philippines, where Paytaca is onboarding merchants and users together after St. Kitts showed what happens when you onboard only the merchants. Europe's crypto payment rails, GoCrypto included, were killed by MiCA's licensing regime rather than by technology. What has not materialized is demand at scale: measured throughput has spent most of nine years far below what the block limit allows, so the capacity argument has largely been tested in theory.

WHO IS WHO

THE BUILDERS



Amaury Séchet("deadalnix")

Lead developer of Bitcoin ABC and the engineer behind the UAHF. He launched Bitcoin Cash, but currently he no longer steers it. His Infrastructure Funding Plan, an 8% coinbase tax routed to his own team, split the community in 2020, and his chain is now eCash XEC. The people who worked with him describe the episode with something less than fondness. "The Greg Maxwell of big blockers," Culianu called him.



Freetrader

Pseudonymous lead maintainer of Bitcoin Cash Node (BCHN), the client that carried the majority through the IFP split and remains the reference implementation for BCH today.



Jonathan Toomim

Independent developer whose ASERT difficulty algorithm replaced the 2017 DAA in November 2020.



CALIN CULIANU

BCHN developer since fork day, author of the Fulcrum Electrum server (used by Cake Wallet among others, and now serving BTC and Litecoin as well) and a maintainer of the Electron Cash wallet. His stated mission: "complete Satoshi's work," get the chain technically ready to be global money if the moment ever comes, and keep the culture non-toxic. He sold all his BTC for BCH after the fork and says he has no regrets, which at current prices is a statement of principle.



GENERAL PROTOCOLS

(AnyHedge, the first BCH DeFi contract in 2020, and the EXO template stack), Riften Labs (Cauldron DEX), Kyle (FundMe.cash, Bitcoin Cash University), Kallisti (Selene wallet), and, without any claim to completeness, Axel Gembe, Dagur Valberg Johannsson, Andrea Suisani and Fernando Pelliccioni of Knuth.



JASON COX

Bitcoin ABC release manager in the 2017 to 2020 era, now associated with the eCash line.



Jason Dreyzehner

The designer behind much of the recent VM work (limits, BigInt, introspection) and the quantum-resistant vault constructions. Rarely gives interviews.



ROSCO KALIS

Creator of CashScript, the high-level contract language that started as a 2019 university project and now underpins most BCH DeFi. Spends most of his time in the Ethereum world and is candid that "the UTXO model is harder to build on."

THE MONEY AND THE MOUTHPIECES



ROGER VER

"Bitcoin Jesus" to his fans, who spent years evangelizing Bitcoin before becoming BCH's most tireless promoter through Bitcoin.com. Arrested in Mallorca in May 2024 on 10 year old US tax charges, three weeks after publishing the book Hijacking Bitcoin; now under a gag order. Still friendly to the project, by the developers' account, but no longer funding it.



VIABTC (HAIPO YANG)

Which mined the first BCH block, ran the first BCH futures market and gave the chain its first weeks of hashrate.



JIHAN WU AND BITMAIN

The industrial weight behind the large block camp in 2017, influence more often asserted than measured.



CRAIG WRIGHT, CALVIN AYRE AND NCHAIN

Allies in 2017 who became the opposing army in the November 2018 hash war and left with Bitcoin SV. I asked Culianu how it felt to have a man claiming to be Satoshi on his side. "It felt bad. It felt weird." He described the post-fork community as "a ragtag band of rebels" who tolerated Wright because he said the right things about Core, and considers the association, along with the infamous wine glass photograph, the single most damaging thing that happened to the big block cause in its early years.



THE EXCHANGES

Whose decisions decided both later splits: in November 2018 and again in November 2020, the chain that kept the BCH ticker was the one Coinbase, Binance, Kraken and the rest said it was.



R/BTC

The subreddit that became the large block camp's home after r/bitcoin's moderators began removing XT fork advocacy in 2015. Political color, not technical authority, but the two forums shaped the tone of everything that followed. Several current BCH figures told me the Reddit era was so bitter that they initially left the community and only came back later, "in a hazmat suit."



STEVE THURMOND

A BTC maximalist from 2011 to 2023 who switched sides, and the creator of Cash Stamps, paper wallets loaded with a couple of dollars of BCH that he hands to strangers and leaves on top of urinals. Not a developer and cheerful about it. His conversion story, from a man who used to spend bitcoin at Overstock and Newegg until the fees made it pointless, is possibly the most common one you will hear in the big block community.



THE TWO FORKS THAT CAME AFTER

Bitcoin Cash's own history repeats the pattern that created it.

On 15 November 2018 the ABC roadmap (CTOR and OP_CHECKDATASIG) collided with nChain's Satoshi's Vision client, which wanted 128 MB blocks and the original opcodes restored with no other changes. Both sides mined their own chain from block 556,767 and, for a few days, threatened to attack each other's. The ABC chain kept the ticker. The SV chain became Bitcoin SV. Culianu now says CTOR "didn't need to happen" and did not need to be pushed through against nChain's objections; the change was ostensibly about faster block propagation via Graphene, but in his reading it was as much about forcing the nChain people out. Steve Thurmond calls CTOR BCH's own humiliation ritual, while noting that ABLA is not in the whitepaper either.

On 15 November 2020 the fight was over money rather than opcodes. Bitcoin ABC wrote its Infrastructure Funding Plan into consensus at what Culianu describes as "the eleventh hour," redirecting 8% of every block reward to a development address without any community process. Bitcoin Cash Node and the other clients refused. "We quickly scrambled to form another dev team, told all the miners which software to install, and he got the boot." Hashrate and exchanges followed BCHN; ABC's chain traded as BCHA and rebranded as eCash (XEC) on 1 July 2021, with 1 BCHA redenominated as 1,000,000 XEC. Several people told me this was the split that made them give up on BCH for a while. The price hit an all-time low of about 75 USD a month after the BSV split and was ranked 35th by market capitalization. Both fork chains have their own articles covering this issue.

WHAT BITCOIN CASH PROVED

The market decides tickers, not developers. Twice, the BCH name went to the chain exchanges chose, and the losing side had to rebrand.

Bitcoin borrowed from it. Jeremy Rubin told me his CTV and CSFS proposals were inspired by an existing BCH opcode called CHECKDATASIG. The WabiSabi paper behind Wasabi Wallet 2.0 cites CashFusion, which shipped on BCH first. Bitcoin Core is working toward UTXO commitments, which BCH has argued for since the node debate began. And in September 2018, at the absolute height of the fork wars, a BCH developer known as Awemany found a live inflation bug in Bitcoin Core (CVE-2018-17144, introduced by a block validation optimization) and disclosed it responsibly. Bitcoin's 21 million owes a debt to a big blocker. Core has never had a reciprocal disclosure agreement with BCHN, and Culianu is no longer sure he would be so polite a second time.

Big blocks alone do not create demand. This is the finding that BCH's own advocates find hardest to argue with, and the one that Bitcoin's small block camp cites most often.

A contentious chain split with proper replay protection can produce a durable, liquid asset. Every later Bitcoin fork copied BCH's SIGHASH_FORKID approach or something like it.

Scheduled hard forks are a viable governance model, at least for a chain small enough that its stakeholders can coordinate. Six consecutive May upgrades have gone off without a split since 2021, and the community's own claim, that no figurehead remains to decapitate, has been tested twice and held.



WILL BCH FLIP BITCOIN?

This magazine's scorecard asks this question for every fork, so let's answer it plainly. At about 0.3% of Bitcoin's market value and about 0.3% of its difficulty, Bitcoin Cash is not on a trajectory to overtake Bitcoin... and nothing in its present market structure suggests otherwise. Even its most committed developers do not claim it is. Culianu's own theory of victory is that the people he calls "the money printer people" will be too busy fighting other fires to bother with a chain this small, and that being under the radar is a feature for now: "It would actually be really dangerous if BCH got to number two right now." A flip would require a reversal in hashrate allocation, fiat rails and social consensus of a kind that no protocol upgrade can deliver on its own. Where BCH's claims do hold up is narrower and real: it is cheaper to use, it has features Bitcoin has declined to adopt, and it is still here, which is more than most 2017 forks can say. The ultimate test of an open source project is whether people keep joining after the big money and the famous names leave. By that measure it passed. Treat flip talk as advocacy, then treat survival as the accomplishment.

SCORECARD INPUTS

CRITERION	EVIDENCE
Technical ambition	8 MB to 32 MB to adaptive; CTOR; Schnorr in 2019; native tokens; introspection; unbounded integers; loops. Deliberately non-SegWit, non-Taproot
Political radicalism	Contentious split against the SegWit majority, then two further contentious splits within its own camp
Adoption	Continuous listing on all major exchanges since 2017; market cap about 0.29% of BTC (17 Sept 2026); merchant pockets in Australia, Argentina and the Philippines; European rails lost to MiCA
Scalability claims vs measurement	Fees consistently a fraction of Bitcoin's; sustained throughput far below the block limit for most of its history
Decentralization	Several independent node implementations; counterweight of higher node costs at full capacity and historically concentrated advocacy
Security model	Same SHA-256d assumptions as Bitcoin at about 0.33% of the difficulty; no merge mining; first hostile attack attempt in May 2026 failed; structurally exposed to rented hashrate
Long-run viability	Active CHIP process and annual upgrades; developers still joining post-2020; repeated splits and nine years of relative decline against BTC
Speculative context	Upside: payments and CashTokens applications if on-ramps deepen. Downside: permanent minority-hash status, brand lock-in to BTC, split fatigue

Sources

UAHF Technical Specification and the 2017 to 2026 upgrade specifications (upgradespecs.bitcoincashnode.org); mempool.space API for block 478,558 (header time 1501593374); CoinDesk and Bitcoin.com News coverage of 1 August 2017; reference.cash for the May 2023 upgrade; CoinGecko API and coin page for market data, 17 September 2026; Coin Dance BCH statistics, 17 September 2026; Decrypt on the November 2020 split; bitcoinabc.org on the BCHA to XEC rebrand; bitcoincashnode.org team page; Internet Archive capture of bitcoincash.org from December 2017; Bitcoin Takeover Podcast S17 E26 (27 May 2026), interviews with Calin Culianu, Steve Thurmond, Rosco Kalis, Kallisti, FiendishCrypto, Kyle and others.


BLAKE2B
BLAKE2b
THE FORK THAT FIRED THE MINERS



BIP-110

THE SOFT FORK THAT WANTED A SMALLER BITCOIN

The story begins with a grievance that has nothing to do with block size, at least on its surface. Since the **Ordinals wave of 2023**, a vocal part of Bitcoin's community has regarded inscriptions, large OP_RETURN outputs, and other non-monetary data as spam that burdens node operators and crowds out payments. Bitcoin Core disagreed, and in 2025 it went the other way, **loosening its OP_RETURN policy**. Bitcoin Knots, the alternative client Luke Dashjr has maintained for over a decade, became the home of the opposition.

Kurt Wuckert Jr told me on S17 E39 that his own political awakening came from the same wound, from the other direction. Around 2014 his OP_RETURN tokenization prototype stopped working when Core **cut the data carrier size**, and his first reaction was to go looking for who this Luke Dashjr person was. A decade later, the anti-data camp and the pro-data camp were both still fighting over the same 80 bytes.

BIP-110, the "**Reduced Data Temporary Softfork**," was written by Dathon Ohm and credits Luke for the original draft. For about a year, it would have limited new output scripts to 34 bytes (OP_RETURN to 83), capped data pushes at 256 bytes, banned the Taproot annex, deep control blocks, OP_SUCCESS opcodes and OP_IF inside Tapscript, and grandfathered all existing coins. Activation needed 55 percent of miners signaling on bit 4. If they refused, Knots nodes would begin rejecting every block that did not signal at height 961,632.



They refused. Signaling peaked at 2.53 percent. On **8 August** the mandatory period began, Knots nodes rejected the next block the majority mined, and the chain split. More than **99 percent of hashrate** stayed on Bitcoin. The minority chain inherited Bitcoin's full difficulty, which meant it needed roughly Bitcoin's hashrate to produce a block every ten minutes. It produced two blocks in eight hours and then almost nothing: the Roughnecks pool mined four in the first week, then single blocks arrived on 17, 21, 23 and 28 August. The last, tagged OCEAN, came from the pool Luke co-founded, which had pointed its customers' hashrate at the minority chain for about 18 hours without clear consent. OCEAN's hashrate **fell 96 percent** in August. Its customers demanded new leadership, and on 29 August Luke resigned as chairman, CTO and director, with OCEAN buying back his equity.

The stalled chain also had **no replay protection**. By mid-August more than **400,000 transactions** were sitting in its mempool, most of them ordinary Bitcoin transactions that users had broadcast **without realizing** they were valid on both chains.

Bitcoin's developers moved faster than its miners. On 9 August **Mark "Murch" Erhardt** filed a motion to remove Luke as a BIP editor, citing his central role in "***a new forkcoin spun out of Bitcoin under his leadership.***" The other editors approved it within days. Luke's reply: "***They have no authority to do so***." The official BIP-110 document was marked Closed "***following a chain split with stalled mining***." The advocacy site bip110.org, meanwhile, still says BIP-110 "***has been activated at the block height 961632 on 8 August 2026 successfully***." Both statements are technically true, which tells you everything about how this fork uses language.



How **Luke Dashjr's** anti-spam soft fork won 2.53 percent of the hashrate, died in eight blocks, came back with a new proof of work chosen by lottery, and now wants to lock its own miners' rewards for 45 days

In May, eight hours into my Bitcoin Cash marathon with Calin Culianu and Steve Thurmond (S17 E26), the conversation drifted toward Luke Dashjr. Someone asked whether I agreed with the fork he was threatening to unleash. I said I didn't: "***If you want to fork off, at least add something that's technologically interesting. He's going backwards.***" I even added the detail that made the room laugh: "**He wants 333 kilobytes**." Calin, who maintains Bitcoin Cash Node, was less polite. "***I can fork Bitcoin Core tomorrow. It's not that hard. It's like 95 percent the same code anyway***."

Three months later Luke **forked Bitcoin**, and the blocks on his chain are capped at about **300 kilobytes**. I had been wrong about one thing: the fork does contain something technologically interesting. It just arrived wrapped in the strangest governance I have covered in this magazine. The new proof-of-work algorithm was **picked by lottery**, where the last hex digits of Testnet4 blocks sealed the project's fate. Activation required a New York Post headline in the coinbase: "***blake2b_headline=8-30 NYPost Deride and Conquer***". Its developers call the chain they left "Spamcoin" and the exchanges that list it "incompetent." Now the fork is going after its own miners.

Of every chain in this issue, this is the youngest and the most volatile, and it may prove the most short-lived. It is also the only one that began as an attempt to make Bitcoin smaller and less scalable. Which is ironic, as so-called Bitcoin maximalists are trying to minimize the design.



VITAL STATISTICS

Snapshot data from 17 to 21 September 2026. This chain changes weekly, so read every figure with its date.

FIELD	VALUE
Names	Bitcoin BLAKE2b, Bitcoin BIP110, BTCB2, XBT; the project itself also says BIP110, and Luke Dashjr calls it BTC
Category	UTXO hard fork of Bitcoin with a new proof of work; every BTC holder at block 961,631 holds the same balance on this chain
Last common block	961,631, mined 8 August 2026 at 19:33:48 UTC
Split	961,632 at about 20:12 UTC on 8 August, the first block of BIP-110's mandatory signaling period
SHA-256d stall	Eight blocks (961,632 to 961,639) in 22 days, the last one tagged OCEAN on 28 August
First BLAKE2b block	961,640, 30 August 2026 at 06:14 UTC, mined by SilentWave
Proof of work	BLAKE2b with a 164-byte version-2 header; Bitcoin's 2,016-block retarget kept
Temporary rules	Reduced-data rules and an 800,000 weight unit cap (about 300 kB) until 1 September 2027
Client	Bitcoin Knots 29.4.1.knots20260508
Supply	Same 21 million cap and halvings; 20,067,600 coins at the split; next halving at block 1,050,000
Coinbase maturity	100 blocks, rising to 6,480 blocks (about 45 days) for rewards mined from 973,440 to 979,920
Hashrate	About 17 PH/s of BLAKE2b across 27 pools (8 September); not comparable with Bitcoin's SHA-256d exahashes
Height	972,506 on 17 September, about 5,170 blocks ahead of Bitcoin
Price	Peak $1,799 (5 September); $270 to $315 (21 September)
Market cap	Not listed on CoinGecko or CoinMarketCap; no meaningful figure exists

THE LOTTERY, THE HEADLINE AND THE REHEARSAL

A chain that cannot attract **SHA-256 miners** has one way out: stop needing them. On 10 August, at a Bitcoin Knots development meeting on the **project's official Discord**, supporters divided up the work. Luke took the new block header and proof of work. A developer known as **Kyle** took replay protection. **Chris Guida**, who had already updated a proof-of-work change plan Luke wrote in 2017, took the job of carrying BIP-110's rules into the new chain.

The algorithm itself was **chosen by lottery**. On 11 August Knots ran a commit-reveal process on Testnet4 to pick among six candidates: **BLAKE2b-256**, **SHA3x**, **BLAKE2s**, **Scrypt**, **BLAKE3x2** and **Eaglesong**. **BLAKE2b** won the next day. The choice mattered, because BLAKE2b is the algorithm of Siacoin, which means a secondhand market of ASICs (Bitmain's Antminer A3, Goldshell's SC5 and SC Lite) already existed. Peter Todd accused Luke of choosing Testnet4 for the draw because its blocks are easy to manipulate, and pointed out that people close to the fork, such as the account **@BitcoinSith**, showed off freshly acquired BLAKE2b machines barely a week later, when delivery normally takes two to three weeks. That is Todd's allegation, not a finding, but it is the kind of question a proof of work chosen by dice invites.

Then came the **rehearsal**. On 29 August Luke asked the remaining SHA-256 miners to stop, and release candidate rc4 was set to mark the last SHA-256 block. On 30 August he published the parameter that would seal ***activation: blake2b_headline=8-30 NYPost Deride And Conquer***. The first BLAKE2b block had to carry that day's New York Post headline in its coinbase, echoing the Times headline Satoshi placed in Bitcoin's genesis block. SilentWave mined it at 06:14 UTC. Within two hours SilentWave, PyBLOCK, Helios, PythonPool, TrueNorth, Connor's Lab and a solo miner had produced fourteen more, each just under the new 800,000 weight unit cap. The rehearsal became the launch, and the final Knots release followed on **2 September**.

WHAT CHANGED AT THE FORK

The BLAKE2b hard fork is not BIP-110. The project's own FAQ says so, and the distinction matters: BIP-110 was a temporary soft fork; this is a permanent new chain.

1

A new proof of work

BLAKE2b replaces SHA-256d from block 961,640. Every Bitcoin ASIC in the world became useless on this chain overnight.

2

A 164-byte header

Bitcoin's header is 80 bytes. The new one adds the block height, a transaction count, larger nonce fields, ASIC profiles, time-offset data, an XOR key and a field reserved for merge mining.

3

A transaction-count commitment

Committing to the number of transactions in the header closes the Merkle tree ambiguity behind CVE-2017-12842, a fix Bitcoin Cash already has and Bitcoin still lacks.

4

Block-withholding protection

A pool can hash with a secret XOR key so its workers cannot tell when they have found a valid block and quietly withhold it.

5 Opt-in replay protection

SIGHASH_UNIFIED (bit 0x20) commits to every input amount and works across legacy, SegWit and Taproot inputs. It only protects users who choose it; ordinary signatures remain valid on both chains.

6 The reduced-data rules

BIP-110's restrictions apply until the parent block's median time passes 1 September 2027, alongside a block weight cap of 800,000 units, about 300 kB. Luke has wanted smaller blocks since at least 2017, when he proposed cutting Bitcoin's base block to 300 kB. He now has them.

7 A low starting difficulty

The initial target was set for roughly 218 TH/s. Because far more BLAKE2b hashrate arrived than that, blocks came in seconds until the 2,016-block retarget caught up, four times harder at each step. That is why this chain is now thousands of blocks ahead of Bitcoin.

Addresses, keys, ports and the network magic were not changed. A BTCB2 address looks exactly like a Bitcoin address, so exchanges have to identify the chain by its fork-anchor hashes, not by appearance.

TIMELINE

DATE	EVENT
Jul 2026	Adam Back calls BIP-110 “idiocracy”; signaling hovers around 1 to 2 percent
8 Aug	Mandatory signaling begins at 961,632; chain splits at 2.53 percent peak support
9 to 10 Aug	Motion to remove Luke as BIP editor; Knots Discord meeting assigns hard fork work
11 to 12 Aug	Commit-reveal lottery on Testnet4 selects BLAKE2b from six candidates
15 Aug	Minority chain stalled at 961,635; more than 400,000 replayed transactions waiting
28 Aug	Last SHA-256d block, 961,639, tagged OCEAN
29 Aug	Luke resigns from OCEAN; SHA-256 miners asked to stop
30 Aug	BLAKE2b activates at 961,640 with the New York Post headline in the coinbase
2 Sep	Final Knots 29.4.1 release
~2 Sep	First trades on Neoxa as BTCB2 around $80, on a 131.7 percent bid-ask spread
5 Sep	Peak at $1,799
8 Sep	Neoxa renames it XBT; Alphapool passes 50 percent of hashrate; blacklist patch appears
15 Sep	Luke opens Knots PR #419, “Long coinbase maturity”
21 Sep	PR #419 merged; price $270 to $315
22 Sep	45-day maturity window begins at block 973,440
1 Sep 2027	Reduced-data rules and 300 kB cap scheduled to expire

WHERE IT TRADES

No major exchange lists the coin, and neither CoinGecko nor CoinMarketCap tracks it. Everything that exists trades on three small venues, each under a different name.

Venue	Ticker	Pairs	Notes
Neoxa / NeoxEX	XBT (since 8 Sep; the market URL still reads BTCB2_USDC)	USDC, USDT, BTC	First venue; about USD 916,000 in 24h volume on its USDC book on 8 September; publicly endorsed the 45-day maturity soft fork
NonKYC	BTCB2	USDT, BTC	Internal record names the asset "Bitcoin BIP110 (BLAKE2b)"; about $280,000 in 24h volume on 17 September
SafeTrade	BIP110 and XBT	USDT	Very thin; the BIP110/USDT market has at times shown as disabled

A naive calculation (20 million coins times $300) produces a market cap of about USD 6 billion. It is meaningless. A handful of order books with six-figure daily volume cannot price 20 million coins, most of which have never moved since the split and belong to people who do not know or care that they own them.

Neoxa's own debut was chaotic. A pro-BIP-110 website published a warning that it was "a high-risk, unverified custodial exchange," and Neoxa's staff answered by threatening to delist the coin over the controversy. Within a week it was the fork's main market.

THE WAR WITH THE EXCHANGES

Every fork in this magazine eventually fights about its name. This one fought about its name before it had a price.

Luke's position is that nothing was forked away from Bitcoin at all. "*There's no reason for Bitcoin to change its name,*" he wrote in August, and he has since published a timeline of Bitcoin's history in which the majority chain becomes "**Spamcoin**" from 8 August 2026. On X he argues that the BTC ticker has belonged to Bitcoin for over a decade, and Bitcoin has now moved to **BLAKE2b**. When Swan co-founder Yan Pritzker asked whether he really believed exchanges don't run their own nodes, Luke answered that competent operators would never have listed the SHA-256 chain: "*If they did, they wouldn't be selling fake bitcoins now. Unless you're saying it's intentional fraud.*" Chris Guida has told supporters to avoid KYC exchanges entirely and acquire the coin through goods and services.

The exchanges were unmoved. Not one venue agreed to list the fork as BTC. Neoxa's explanation was simple: "*We didn't use BTC because we already have a BTC ticker on the exchange.*" Instead it used XBT, the ISO 4217-style code Kraken and much of the institutional world have used for bitcoin for years. That produced its own backlash. *"XBT is the ISO-compliant currency code for Bitcoin,*" wrote Coinjoined Chris of Seedor and Bitsurance fame. "*Blake Bitcoin is not Bitcoin is not XBT*." Neoxa replied that "*projects choose tickers," that the team had asked for XBT, and that it had done its due diligence and "there was nothing illegal about calling it XBT.*" The project also uses an old version of the Bitcoin logo.

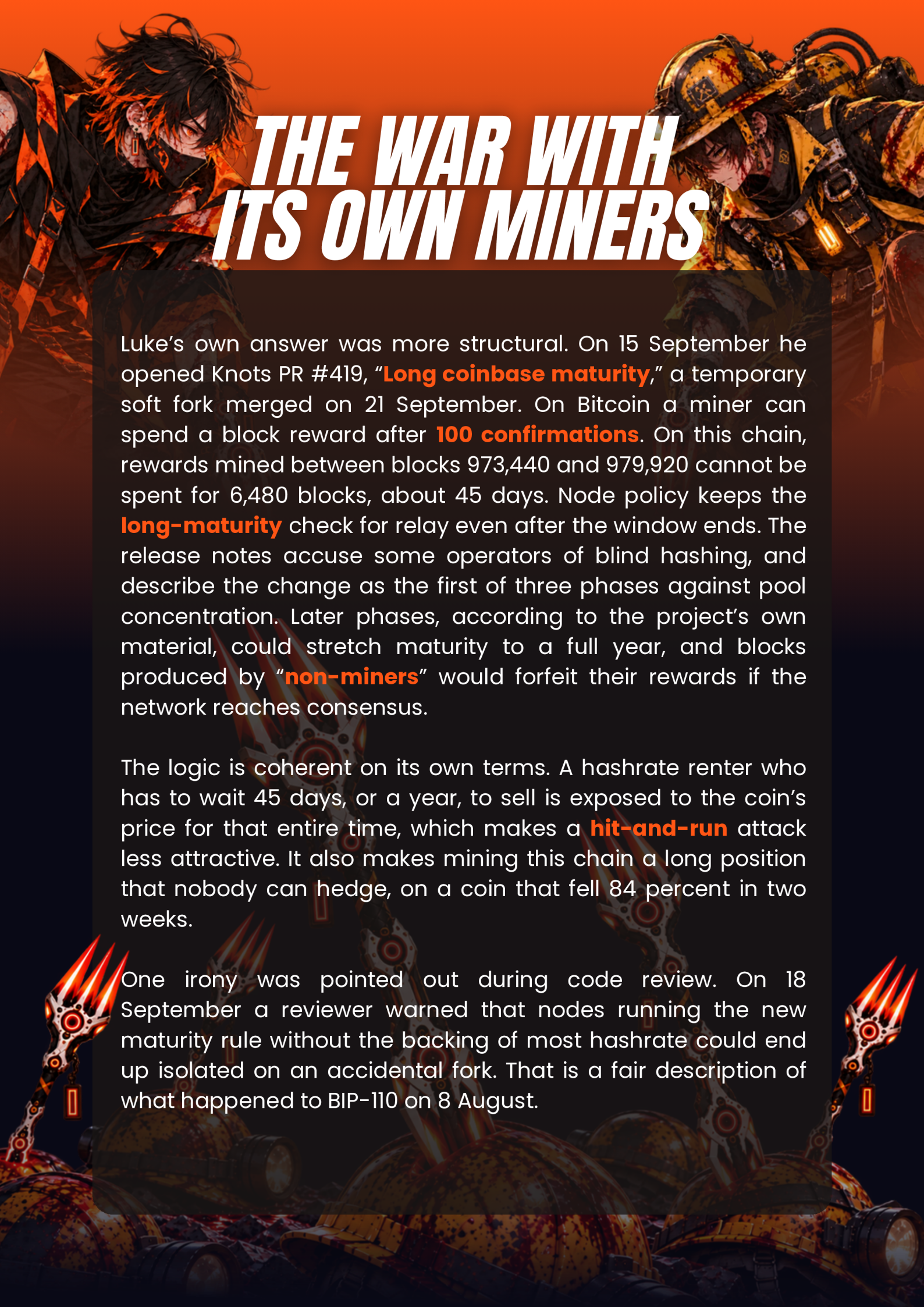
So the same asset now answers to BTCB2, XBT, BIP110, "**Bitcoin BLAKE2b**," "**Bitcoin BIP110**" and, according to its founder, BTC. That is not a branding problem, but an outright operational hazard: the addresses are identical to Bitcoin's, and the ticker on at least one exchange is a synonym for Bitcoin's own.

THE WAR WITH ITS OWN MINERS

The fork's founding complaint was that Bitcoin's miners refused to enforce rules its users wanted. Its first month showed that the complaint travels.

In the vocabulary of this camp, a miner is whoever builds the block template, meaning chooses the transactions. Someone who points an ASIC at a pool and hashes whatever the pool hands them is not really mining. They are "**blind hashing**." This is why the fork's mining stack is built around DATUM, the **OCEAN-developed** protocol that lets individual miners build their own templates, and why several pools now subsidize it. Lazarus Pool raised its public stratum fee from 15 to 25 percent from block 973,750, giving half of the increase to miners who run their own **DATUM gateway**.

On 8 September one pool, Alphapool, briefly controlled more than half of the fork's hashrate. On the **Knots Discord**, supporters argued over whether that was an attack or just miners chasing cheap blocks. Some told Alphapool on X to "**stop mining**." A proposal appeared on GitHub to blacklist Alphapool's payout address at the consensus level, which would have made its blocks invalid. Luke labeled that patch "**DO NOT RUN THIS CODE**." Alphapool, bewildered, wrote: "*Never in all my years have I seen submitting hashrate and securing a blockchain protocol in and of itself perceived as a 'hostile attack.*'" In the same Discord it promised to cap itself at 30 percent of network hashrate and refuse new connections above that. By the afternoon it had fallen below 18 percent.

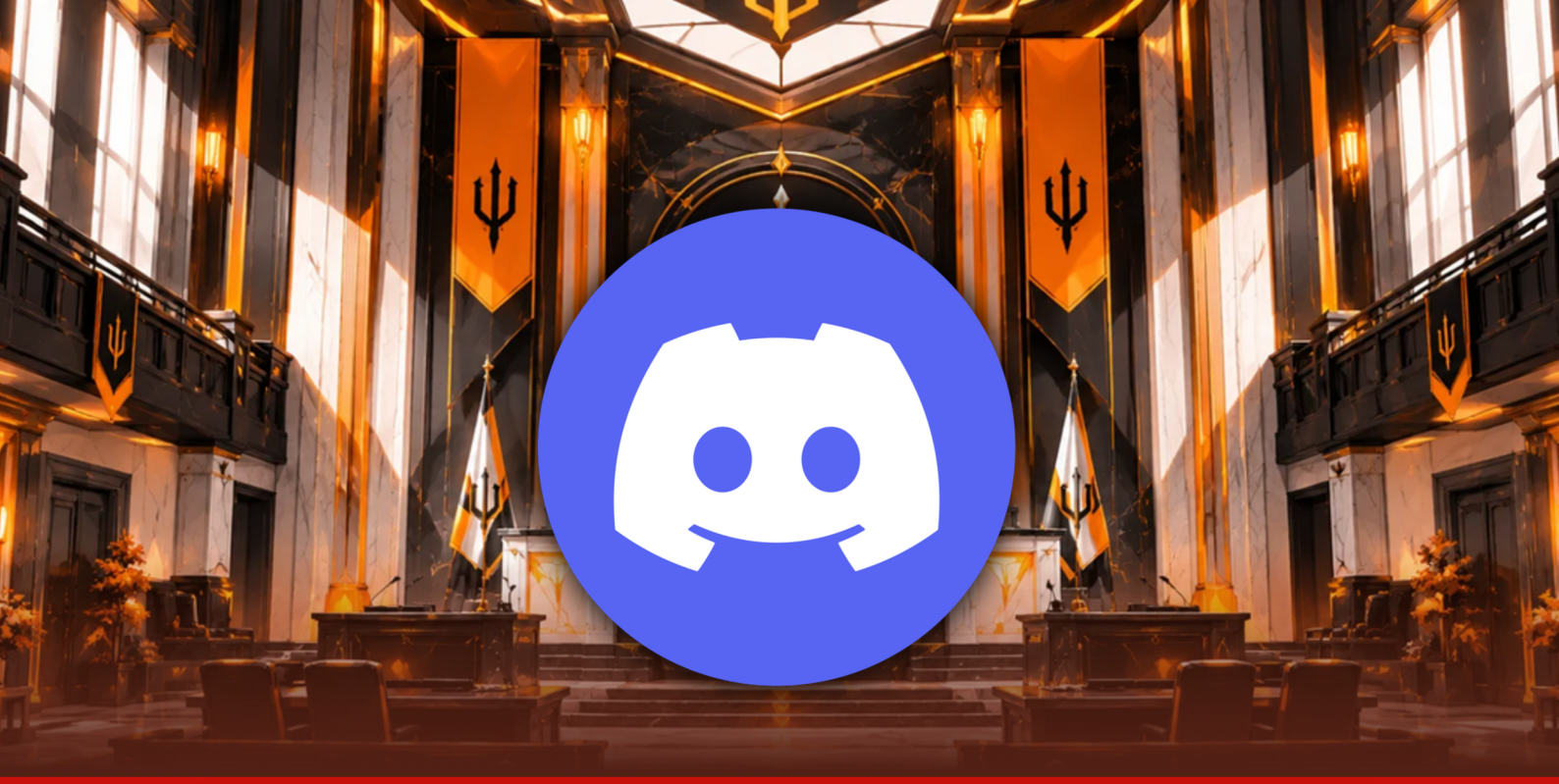


THE WAR WITH ITS OWN MINERS

Luke's own answer was more structural. On 15 September he opened Knots PR #419, "**Long coinbase maturity**," a temporary soft fork merged on 21 September. On Bitcoin a miner can spend a block reward after **100 confirmations**. On this chain, rewards mined between blocks 973,440 and 979,920 cannot be spent for 6,480 blocks, about 45 days. Node policy keeps the **long-maturity** check for relay even after the window ends. The release notes accuse some operators of blind hashing, and describe the change as the first of three phases against pool concentration. Later phases, according to the project's own material, could stretch maturity to a full year, and blocks produced by "**non-miners**" would forfeit their rewards if the network reaches consensus.

The logic is coherent on its own terms. A hashrate renter who has to wait 45 days, or a year, to sell is exposed to the coin's price for that entire time, which makes a **hit-and-run** attack less attractive. It also makes mining this chain a long position that nobody can hedge, on a coin that fell 84 percent in two weeks.

One irony was pointed out during code review. On 18 September a reviewer warned that nodes running the new maturity rule without the backing of most hashrate could end up isolated on an accidental fork. That is a fair description of what happened to BIP-110 on 8 August.



GOVERNANCE BY DISCORD

For a movement that exists because it believes Bitcoin Core makes decisions without real consensus, the fork's own decision-making has been unusually informal. The work plan was divided in a Discord meeting. The proof of work was drawn by lottery. The activation block was defined by a newspaper headline posted on X. The response to a dominant pool was debated in Discord, and the pool's promise to limit itself was made in Discord too. The planned rule under which "non-miners" lose their rewards applies only "if the network reaches consensus," and I could find no public document explaining how that consensus will be measured, who counts as a non-miner, or who decides.

This is not unusual for a chain six weeks old. It is unusual for a chain whose founders call the other side "**centrally managed**."

HOW IT DIFFERS FROM BITCOIN TODAY



CONSENSUS

The two chains share every block up until **961,631**. After that, this chain has a different proof of work, a different header, temporary data restrictions, a **300 kB block cap**, opt-in unified signatures and, from 22 September, a 45-day coinbase lock. Its script system is otherwise Bitcoin's, including **SegWit and Taproot**, but with Taproot's extension points switched off during the reduced-data window.

ON SCALING

Every other fork in this issue wanted more room: **Bitcoin Cash**, **Bitcoin SV** and **eCash** with bigger blocks, Bitcoin Gold with fairer mining. This is the first to want less. Blocks are a third the size of Bitcoin's base block, and the explicit goal is block space for money only. Tip blocks I have observed so far carry anywhere from a dozen to a little over a thousand transactions.

ON SECURITY

Changing the proof of work did what it was supposed to do: Bitcoin's ASIC fleet can **no longer attack** this chain, or support it. The fork is now defended by roughly **17 PH/s of BLAKE2b**, a figure that means little to anyone outside the Siacoin market, and by a pool ecosystem in which one operator could, and briefly did, command a majority. The 45-day maturity is the fork's answer to rented hashrate. Bitcoin Gold's experience in this magazine **suggests that exchanges** will also demand very deep confirmations.

HOW IT DIFFERS FROM BITCOIN TODAY



ON DECENTRALIZATION

One client, Knots, maintained by the person who designed the fork, chose its algorithm, announced its activation string and wrote its maturity rule. The miner base is new, enthusiastic and concentrated. The project's answer is **DATUM**: many small miners building their own templates. Whether that holds when the coin is worth less than the electricity is the next test.

ON ADOPTION

Three **small exchanges**, **three tickers**, **no aggregator listing**, and **no wallet support** beyond Knots itself and a few community projects. The fork's leaders are openly hostile to the exchanges that would normally bring liquidity, and those exchanges have shown no interest in coming.



WHO IS WHO

THE FORK

Luke Dashjr

Maintainer of Bitcoin Knots and one of Bitcoin's earliest contributors. Credited on BIP-110, author of the BLAKE2b header, the activation headline and the coinbase maturity rule. Removed as a BIP editor and resigned from OCEAN in August; now leads CONVOY Mining. Calls the original majority chain Spamcoin.

Chris Guida

Developer who updated the 2017 PoW change plan and ported BIP-110's rules to the new chain; the most outspoken voice against KYC exchanges.

Dathon Ohm

Author of the BIP-110 specification.

Kyle

Developer assigned replay protection at the 10 August meeting.



Loogart

Supporter whose X exchange with David Schwartz became the fork's most quoted defense: "We accepted that we lost the attempt to fix the legacy chain, so we continued Bitcoin elsewhere."

SilentWave

Miner of the first BLAKE2b block.

Alphapool

The largest pool by hashrate, briefly above 50 percent; now self-capped at 30 percent.

Lazarus, PyBLOCK, Mycology, Pow.re, XorPool, Blockvase and others

The 27-odd pools and solo miners of the first month.

Neoxa

The exchange that listed the coin first and renamed it XBT.

WHO IS WHO

THE OTHER SIDE



Bitcoin Core and the BIP editors

Led in this episode by Mark “Murch” Erhardt, who filed the motion to remove Luke.

OCEAN

The pool Luke co-founded, which lost 96 percent of its hashrate after sending customers’ work to the minority chain.

Adam Back

Blockstream CEO: BIP-110 was “idiocracy” in July, and after the split, “Live by the fork, die by the fork.”

David Schwartz

Ripple’s former CTO, to Loogart: “You switched from participating in governance to attacking when you refused to accept that you lost.”

Coinjoined Chris

Who led the protest against the XBT ticker.

Peter Todd

who accused the PoW lottery of being rigged by incompetence and malice.

WHAT BITCOIN BLAKE2B PROVED

FIRING THE MINERS DOESN'T END THE ARGUMENT WITH MINERS

Within six weeks the chain that left Bitcoin over miner power was fighting a dominant pool and drawing up rules to take rewards from "non-miners."

A user-activated soft fork without miners is a hard fork with extra steps. At 2.53 percent support, mandatory signaling did not enforce anything on Bitcoin. It created a second chain and stranded its users' transactions.

YOU CAN CHANGE BITCOIN'S PROOF OF WORK IN THREE WEEKS

From the lottery on 11 August to the first BLAKE2b block on 30 August took nineteen days. Whatever else you think of this fork, that was a fast piece of engineering.

THE HEADER CAN BE FIXED

The transaction-count commitment and the XOR key address real, known problems in Bitcoin's design that Core has not addressed.

THE MARKET DECIDES THE TICKER

No exchange agreed to call this chain BTC, just as no exchange agreed to call Bitcoin Cash or Bitcoin SV by that name.

HOLD YOUR FORKS

If you held Bitcoin in self-custody on 8 August, you own this coin under your existing keys. Anyone asking for your seed phrase to "claim" it is a thief.



WILL IT FLIP BITCOIN

No. The fork has **no aggregator listing**, three thin order books under three different names, a hashrate measured in a different unit from Bitcoin's, a single-client governance model, and a price that **fell 84 percent** in its first three weeks. It also has something every other fork in this issue lacked at birth: a founder with fifteen years of Bitcoin development behind him and a following that genuinely believes the majority chain has been captured.

The honest verdict comes in two parts. As a **claim to be Bitcoin**, it is already over; the exchanges have spoken, and so has more than **99 percent of the hashrate**. As an experiment, it is barely six weeks old, and the questions it asks are real: whether a small, data-restricted chain can keep miners honest by locking their rewards, and whether template-building miners can replace pool operators. Treat flip talk as advocacy. Watch block 979,920.

SCORECARD INPUT

CRITERION	EVIDENCES
Technical ambition	New PoW chosen and deployed in 19 days; 164-byte header with tx-count commitment and XOR key; SIGHASH_UNIFIED; long coinbase maturity. Real engineering on a rushed schedule
Political radicalism	Mandatory signaling at 2.53 percent support; “Spamcoin”; exchanges accused of selling “fake bitcoins”; consensus blacklist proposed against a pool; planned reward forfeiture for “non-miners.” The most radical governance posture in this issue after BSV
Adoption	Neoxa (XBT), NonKYC (BTCB2), SafeTrade (BIP110/XBT); no CoinGecko or CoinMarketCap listing; no major exchange
Scalability claims vs measurement	Explicitly anti-throughput: 300 kB blocks until 1 September 2027
Decentralization	Single client and single lead developer; one pool briefly above 50 percent; DATUM template-building as the proposed remedy
Security model	About 17 PH/s of BLAKE2b, drawn from the Siacoin ASIC market; immune to SHA-256 ASICs; 45-day maturity against rented hash; replay protection opt-in only
Long-run viability	Continuous blocks since 30 August; active development; three-phase miner plan. Counter-signals: 84 percent drawdown, ticker chaos, hostility to exchanges, rules expiring in 2027
Speculative context	Upside: a pure-money brand for the anti-inscription camp. Downside: illiquidity, replay losses, mistaken deposits to BTC addresses, and a miner base that may not wait 45 days to be paid

SOURCES

BIP-110 specification and bip110.org; Bitcoin BIP110 technical reference; Bitcoin BLAKE2b FAQ; Bitcoin Knots 29.4.1 release; mempool.guide explorer and mempool.space for fork-anchor hashes; blake2bminer.com block-by-block chronology; awesome-bitcoin-blake; Bitcoin.com News on the revival, the USD 1,799 peak, the XBT ticker and Alphapool fight and the 45-day maturity; Crypto Economy on PR #419; BeInCrypto on OCEAN, Adam Back and the "fake bitcoins" exchange; crypto.news on the 2.53 percent signaling peak and the Schwartz exchange; Observatorio Blockchain on the Discord meeting and PoW lottery; CriptoNoticias on the "Spamcoin" timeline; Odaily on the stalled chain; LeedMiner name map; Lazarus Pool; Jimmy Song on replay and maturity economics; Bitcoin Takeover Podcast S17 E26 (Calin Culianu, Steve Thurmond and guests, May 2026) and S17 E39 (Kurt Wuckert Jr, August 2026).

ECASH (ECX)



PAUL SZTORC

FORKS BITCOIN TO PROVE A POINT



After eleven years of trying to convince Bitcoin to adopt Drivechains, the man who invented them stopped asking. His eCash fork copies Bitcoin's ledger, adds as many sidechains as miners are willing to support, reallocates half of Satoshi's stash, and goes live on Halloween 2026. In many ways, ECX is the most ambitious of all fork in this magazine… and the one Bitcoin developers should watch most closely.

I have known **Paul Sztorc** since 2018, and I have had him on Bitcoin Takeover podcast about 11 times without ever repeating the same interview talking points. So I have watched his work grow and improve over time. What I like about Paul is that he is focused on being **technically correct**, cares about finding the truth, but still finds the time to use funny or interesting metaphors to describe his ideas. When someone objects on the grounds of vibes or personal disagreements, Paul brings the conversation back to objective facts. He doesn't get emotional about technology and he is willing to be proven wrong. Which is something that's truly rare in the space.

Paul Sztorc first described **Drivechains in 2015**, formalized the concept as **BIP-300** in 2017 and **BIP-301** in 2019 alongside his friend BitAxe, and spent the following decade arguing for them in blog posts, conference talks, and podcasts. Then he started a company named **LayerTwo Labs**, used the money to pay his harshest critics (**Peter Todd and Luke Dashjr**) to do professional reviews of his ideas, and then funded developers to build the piece of software that lets miners activate BIP300 without asking permission from Core (**CUSF, or the Core Untouched Soft Fork**). None of it turned out to be fruitful. BIP-300 is still a Draft. So in April 2026, Paul formally announced he was done waiting, and that he would fork Bitcoin himself.

This is the short version of the story about the **new eCash**, whose ticker is **ECX**. It is also the story of a friend who has been right about a remarkable number of things and has too often made it hard for people to notice or acknowledge.

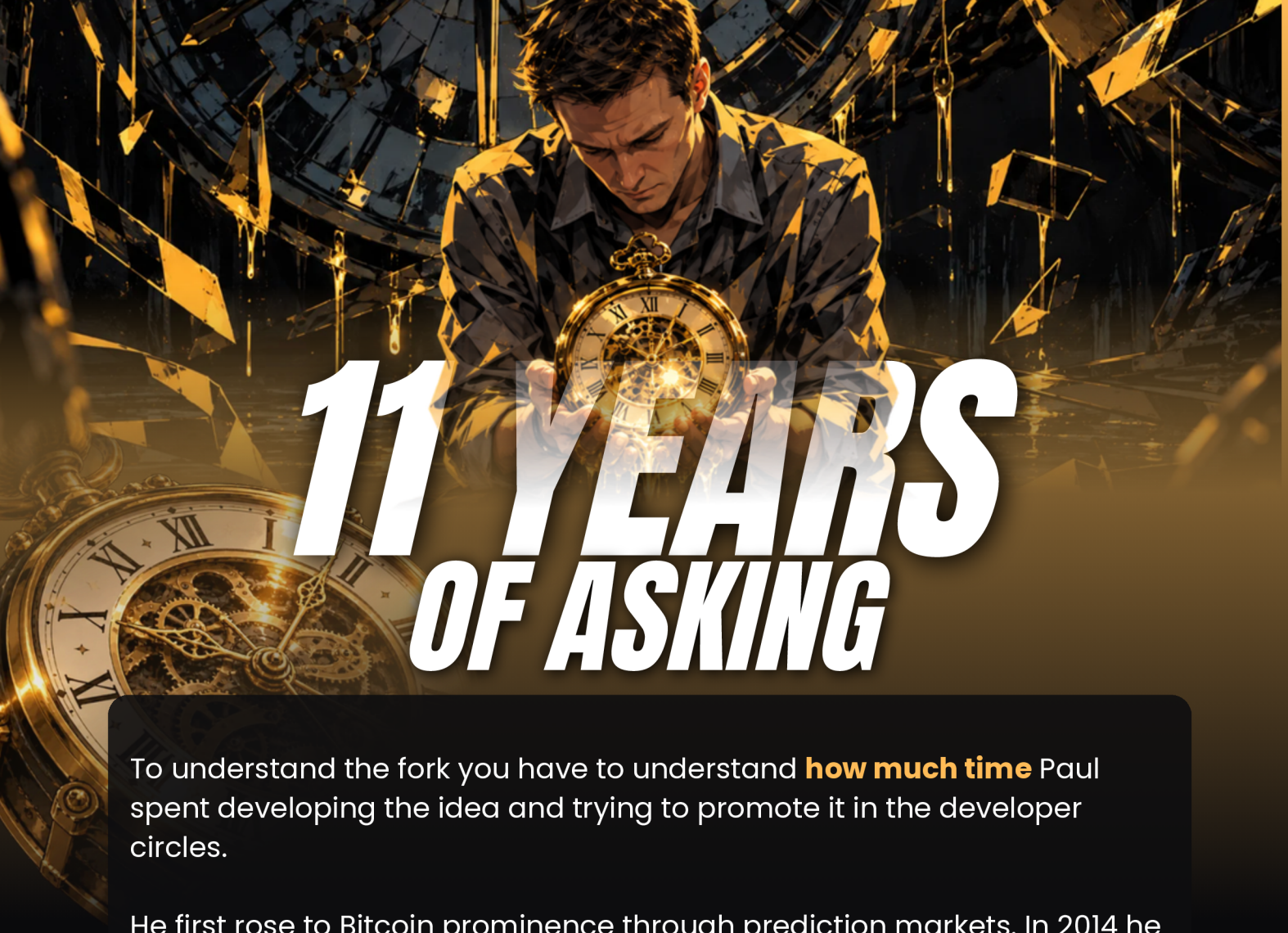
Disclosure: *LayerTwo Labs, Paul's company, sponsors the Bitcoin Takeover podcast and this magazine. I have tried to hold this article to the same standard as the others in the issue. You can judge whether I succeeded.*

VITAL STATISTICS



Data as of 28 September 2026. The permanent chain does not exist yet, so most of these figures describe the rehearsals.

FIELD	VALUE
Name and Ticker	eCash, ECX (practice coins on Alpha and Beta: pECX)
Not to be confused with	eCash (XEC), Amaury Séchet's Bitcoin Cash fork; Cashu and Fedimint ecash; David Chaum's 1990s eCash
Category	UTXO hard fork of Bitcoin, built to activate BIP-300 and BIP-301 natively
Announced	24 April 2026, on X, originally for a single fork near block 964,000 in August
Staged launch	Announced 8 August: Alpha, Beta, then a permanent Mainnet
Alpha	Forked from Bitcoin block 963,647 on 23 August 2026; first Alpha block 963,648 at difficulty 1, coinbase tag /layertree-ecash/
Beta	Fired 19 September 2026, around Bitcoin block 967,680
Mainnet	Around Bitcoin block 973,728, on or about 31 October 2026, the whitepaper's 18th anniversary
Distribution	Every Bitcoin address at the Mainnet snapshot receives ECX 1:1; no claim, no form, no registration
Proof of work	SHA-256d, with a one-time difficulty reset to the minimum at the fork
Node	ecash-com/bitcoin, forked from Bitcoin Core v31.1, plus the bip300301_enforcer companion
Sidechains at launch	Seven Options: Thunder, zSide, BitNames, BitAssets, Truthcoin, Photon, CoinShift
Replay protection	Opt-in and one-directional: ECX transactions with nLockTime = 499999999
Satoshi's coins	220 hard-coded transactions reassign part of the Patoshi-pattern coins on the ECX ledger only; about 600,000 stay, about 500,000 go to pre-launch investors
Alpha hashrate	About 5 PH/s in late August, about 9.7 PH/s on 17 September, roughly 0.001 percent of Bitcoin's
Market	No tracked price. CoinMarketCap has an "eCash (ECX)" page with self-reported supply; pECX trades informally



11 YEARS OF ASKING

To understand the fork you have to understand **how much time** Paul spent developing the idea and trying to promote it in the developer circles.

He first rose to Bitcoin prominence through prediction markets. In 2014 he published the **Truthcoin whitepaper**, later renamed **Bitcoin Hivemind**: a way to run betting markets whose outcomes are decided by a decentralized vote instead of a trusted oracle. In order to scale, it needed a home that was not the Bitcoin main chain. Nobody would let a prediction market clutter Bitcoin's base layer, and rightly so. **Drivechains** were envisioned as that home. A sidechain would hold BTC, run whatever rules its users wanted, and send the coins back to the main chain when they were done, with Bitcoin's miners acting as the custodians.

BIP-300, "**Hashrate Escrows,**" co-authored with CryptAxe, was assigned in August 2017, the same month the big blockers left for Bitcoin Cash. That timing is not incidental. Paul has argued for years that Drivechains were the peaceful answer to the block size war: let the people who want big blocks have a big-block sidechain, pegged to real BTC, and nobody has to fork. BIP-301, "**Blind Merged Mining,**" followed in 2019, so miners could collect sidechain fees without running every sidechain's software.

In December 2022 Paul, CryptAxe and former Kraken executive Austin Alexander launched LayerTwo Labs with a $3 million seed round to build the software. In 2023 Luke Dashjr, of all people, opened a pull request to Bitcoin Core implementing BIP-300 (#28311). It was closed in March 2024 without being merged. That October the company paid Peter Todd, one of Drivechain's most persistent critics, to write a detailed technical analysis. He wrote it, but didn't put much effort into it. Paul eventually spent more time dissecting it than it took for Peter Todd to write it.

By late 2024 Paul had a new plan, which he explained in detail on Bitcoin Takeover Podcast S15 E68: a "Core Untouched Soft Fork," or CUSF. Miners would run a small enforcer program beside an unmodified Bitcoin Core, and if a majority of hashrate did so, Drivechains would activate without a single line entering Core's repository. Critics called it a way around peer review. Paul called it the only way left. His explanation of why is still the best summary of Bitcoin's development pace I have recorded:



> "We used to do a soft fork every six months... in the first like seven to eight year period, we did 16. In the second seven to eight year period, we did two. And one was SegWit, 26 months, and then [Taproot] 40 months. So it's just been getting slower and slower."

Miners did not run the enforcer. So in April 2026, Paul announced the hard fork.



RIGHT, EARLY, AND HARD TO LISTEN TO

I want to be fair to Paul here, because the Bitcoin conversation usually isn't.

He was right that Bitcoin's upgrade pipeline was drying up. Taproot activated in **November 2021**, and nothing has activated since. His own project's website puts it bluntly: "**bitcoin has ossified.**" You can argue ossification is a feature and find virtues in a protocol that doesn't change. But you cannot argue that it isn't happening.

He was right that people wanted more from Bitcoin than Bitcoin offered. Ordinals, Runes, BitVM, Citrea, Spark, the whole 2024 rush toward "**Bitcoin L2s**": every one of them confirmed that users and developers wanted programmability, privacy and scale attached to BTC. Most of them got there through federations or trust assumptions Drivechains were designed to avoid.

He was right about prediction markets. In 2014 they were a libertarian curiosity. By 2024 Polymarket was a household name during an American election. The ecashblog marked the eve of the Alpha with a reunion between Paul and Robin Hanson, the economist whose work started the field. That felt earned.

Paul Sztorc is also right that the argument against Drivechains has often been cultural rather than technical. Peter Todd's critique was technical, serious, but half-baked and excessively paranoid about miners that otherwise have all the incentives to remain honest actors. But a lot of the debate was disappointingly ideological.

However, Paul does not like it easy. Here is how his own fork's website explains the decision to leave:



> "I would prefer not to. But it's not up to me. Other people are damaging the Bitcoin project. Core developers have become timid, self-interested, lazy, and corrupt. Miners have abdicated their duty... Bitcoin culture has many entrenched errors, and is probably unfixable at this point."

It then sums up the cost of the fork: "The downside is small: some drama, plus every Bitcoiner gets some free money."

That is Paul in two sentences. The first is a shot at the people he spent a decade trying to persuade. The second is a genuinely good point, phrased as a taunt. I have seen people who agreed with every technical argument about Drivechains walk away because of paragraphs like that (or tweets that express a similar attitude). I have also seen Paul be patient, generous and funny for three hours on a microphone. Both versions are real. But only one tends to end up in screenshots.

THE SATOSHI COINS

The detail that made the April announcement explode had nothing to do with Drivechains.

Roughly **1.1 million BTC** sit in early coinbase outputs that follow the "Patoshi" mining pattern, and are widely assumed to be Satoshi's. They have never moved. On the ECX ledger, which copies Bitcoin's, they would appear exactly as they are. Paul's plan is to leave about **600,000** of them where they are and use **220 hard-coded transactions**, valid without the original signatures, to reassign about 500,000 to investors who fund the project before launch. His justification was that without early capital, eCash would become a "**zombie project**": half built, underfunded, and quietly controlled by whoever happened to show up.

Peter McCormack called it "**theft and disrespectful.**" Paul's answer was short: "**We do not take any of Satoshi's BTC.**" Technically he is correct. Not one satoshi moves on Bitcoin. Jameson Lopp made the same point, while adding that the marketing seemed designed to provoke. But the objection was never really technical. Bitcoin's culture treats an unspent output as sacred, and Satoshi's outputs most of all. Rewriting their copy on another chain, even a chain nobody is obliged to use, crosses a line many people did not know they cared about until it was crossed.

There is a quiet irony worth noting. In S17 E19, **Amaury Séchet** told me that what alarms him most about Bitcoin today is how casually its developers now discuss freezing Satoshi's coins to defend against quantum computers: "**10 years ago people would laugh in your face. But now apparently it is on the table.**" On Bitcoin itself, the idea of touching those coins went from unthinkable to debatable in a decade. Paul simply did it first, on his own chain, in the open, and put a price on it.

ALPHA, BETA, MAINNET

The original plan was one **permanent fork** on 23 August. On 8 August Paul changed it to three. His stated reasons: rehearse the software, encourage a market for practice coins to find a price, and keep a way to abort if something went badly wrong. He was frank about the risk of bugs in rapidly written, partly machine-assisted code, which he called "**LLM bug chaos.**" No Bitcoin fork in this magazine was launched this cautiously. Bitcoin Cash forked in one shot in 2017, and so did everything after it. But then again, none of them were this ambitious in scope either.

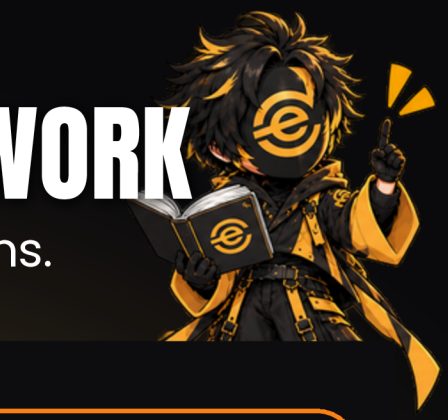
Alpha forked just after midnight UTC on **23 August**, at difficulty 1. The first week ran on rented hashrate, which pushed difficulty up fast. When the rental contracts ended, difficulty stayed high. By **27 August** the network needed about **30.7 PH/s** to produce ten-minute blocks and had about 5. The ecashpool.tech mining dashboard's weather forecast became a community joke: "***mostly slow, chance of drift***." Orphan blocks, a production incident, and a lot of arguing about where to point the hash followed.

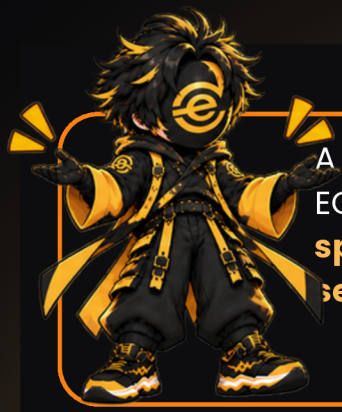
Then came the part that matters for Bitcoin history. During the Alpha, community-built drivechains were activated under **proof of work**, and the first withdrawal bundle was proposed on a live BIP-300 chain. For eleven years Drivechains existed only in documents, testnets and arguments. For a few weeks in **September 2026**, they existed on a chain with real miners and coins that people were willing to buy.

Before Beta, about **150,000 pECX** (practice ecash) were burned by holders. Practice coins from Alpha and Beta are meant to be redeemable for permanent ECX at a steep discount. Paul has been quoted describing a ratio of **1,000 pECX to 10 ECX**. Beta fired on 19 September on schedule. Mainnet is the only stage that creates permanent ECX, from a fresh Bitcoin snapshot around **block 973,728**. That snapshot is what gives every Bitcoin holder their coins. The Alpha and Beta snapshots do not count.

HOW DRIVECHAINS WORK

Here is the idea in plain terms.





A **sidechain** is a separate blockchain that **uses BTC** (here, ECX) as its money. To move coins onto it, you send them to a **special escrow** output on the main chain. The sidechain **sees the deposit** and credits you. That part is easy.

The hard part is **coming back**, because the main chain **cannot read the sidechain's rules**. Drivechains solve this by making miners the judges. When the sidechain wants to release coins from escrow, it publishes a **withdrawal bundle**: one transaction that pays out everyone leaving. Main-chain miners then **vote on it** block by block. **Under BIP-300** a bundle needs **13,150 votes** of approval within a window of **26,300 blocks**, about three to six months. If it gets them, the escrow pays out. *If it doesn't, the bundle expires.*





BIP-301 handles the other half. Sidechain blocks are produced by people who bid for the right to have their block hash included in a main-chain block. Miners collect the bid as a fee without running any sidechain software, which is why it is called **blind merged mining**.

The design choice is the whole argument. There are no fraud proofs and no federation. The coins in escrow are protected by the fact that stealing them would take a majority of miners voting dishonestly, in public, for months, while everyone watches. Supporters say that is the same security Bitcoin already has: miners could always reorganize the chain, and they don't. Critics, Peter Todd foremost, say it turns miners into custodians of every sidechain, adds a new kind of power and liability to mining, and gives them a reason to consolidate. Both sides are describing the same mechanism. For eleven years they could only argue about it. Now there is a chain where the argument can be tested.

THE 7 "OFFICIAL" SIDECHAINS

SLOT	SIDECHAIN	WHAT IT IS FOR
2	**BitNames**	Decentralized names and identity
4	**BitAssets**	Issuing and trading tokens
9	**Thunder**	Large blocks for cheap, high-volume payments
13	**Truthcoin**	Hivemind prediction markets, Paul's original project
98	**zSide**	Zcash-style shielded privacy
99	**Photon**	Post-quantum signatures and vaults
255	**CoinShift**	Swaps between eCash and other coins

Look at that list and you see Paul's answer to the altcoin market. Almost every successful altcoin does one thing Bitcoin won't: privacy, tokens, names, fast payments, quantum resistance. Paul's claim is that each of those should be a sidechain of Bitcoin's money instead of a separate coin with its own supply and its own premine. Truthcoin is on the list because the whole journey started there.

2 FORKS PHILOSOPHIES

The **summer of 2026** produced two serious departures from Bitcoin within weeks of each other, both led by developers with long grievances, and both airdropping coins to every Bitcoin holder. They are opposites in almost every way.

Luke Dashjr's BLAKE2b fork is a conservation project. It exists to remove things: arbitrary data, large scripts, Taproot's extension points, even two thirds of the block size. It changed its proof of work so that Bitcoin's miners could no longer participate, and within weeks it was drawing up rules to punish the miners it did attract. Its idea of Bitcoin is a narrow one: money, and nothing but money.

Paul's eCash is a construction project. It keeps SHA-256d so that Bitcoin's miners can come along. It keeps Bitcoin Core's code almost untouched so it can keep merging Core's changes. Everything new goes into optional sidechains that nobody is obliged to use. Its idea of Bitcoin is a broad one: the most trustworthy money, with every useful feature built on top of it.

The two founders overlap in odd places. Luke wrote a **Core implementation** of BIP-300 in 2023. Both believe Bitcoin Core's process is broken. Both forked in the same month. But when a large pool arrived on Luke's chain, his community debated blacklisting its address at the consensus level. Paul's chain is designed so that miners are paid to be judges. One fork is afraid of what miners might do. The other is betting everything on what they won't.

The eCash community noticed the contrast, not always charitably. In their chat the BLAKE2b chain was promptly renamed "**Lukecoin**," and one member predicted in early September that it "*will probably have its own contentious hardfork within a year. Purity spiral.*" Within days, the puritan fork was fighting over its biggest pool.

ECASH AGAINTS BITCOIN AND BITCOIN CASH

	Bitcoin	Bitcoin Cash	Bitcoin BLAKE2b	eCash (ECX)
Scaling bet	Small base layer, Lightning and other L2s	Bigger base blocks for everyone	Smaller base blocks, money only	Unchanged base layer, opt-in sidechains
Proof of work	SHA-256d	SHA-256d	BLAKE2b	SHA-256d
New features	Rarely, by soft fork	Yearly, by hard fork	Removes features	Mostly off the main chain, via sidechains
Relationship with miners	Miners signal; users enforce	Miners choose the software	Miners distrusted, rewards locked 45 days	Miners judge sidechain withdrawals
Relationship with Bitcoin Core	Is Bitcoin Core	Left in 2017	Left in 2026	Keeps merging Core
Genesis controversy	None	None	Mandatory signaling at 2.53 percent	Reassigned Patoshi coins

Against Bitcoin, eCash is the road not taken: the same chain, the same rules, the same code, plus the one upgrade Bitcoin declined. If Drivechains work, eCash is the proof. If they fail, it is the warning.

Against Bitcoin Cash, the contrast is sharper, because Paul has always said Drivechains would have made Bitcoin Cash unnecessary. Bitcoin Cash made every user carry bigger blocks. Thunder offers large blocks only to the people who choose them, pegged to the main chain's coin. The big blockers of 2017 split the network, the community and the brand to get what Paul argues they could have had as a sidechain. Nine years later he is testing that claim with real money.

THE ECASH MATTERS EVEN IT FAILS

This is the part I hope Bitcoin developers will read.

For a decade, the debate over Drivechains has been about **hypotheticals**. Will miners steal? Will they collude? Will blind merged mining centralize pools? Will anyone use the sidechains? Will withdrawal bundles of thousands of payouts get through in practice? Every one of those questions is empirical, and until August 2026 there was no data, only testnets and blog posts.

eCash is a **free experiment** for Bitcoin. It costs Bitcoin nothing: no code change, no activation, no risk to a single BTC. Its node is so close to Bitcoin Core that its accomplishments will be easy to adopt... if there's ever consensus for it. If miners on eCash honestly approve withdrawal bundles for a year, that is useful feedback for the incentive model. If the miners try to steal, that is good evidence too. If **Thunder** attracts real payments, or **zSide** real privacy users, or **Truthcoin** real markets, this tells Bitcoin something no amount of mailing-list debates can. And the project's own FAQ says it will call itself off if Bitcoin activates **BIP-300 and BIP-301** first, which makes the whole fork a standing offer as much as an exit.

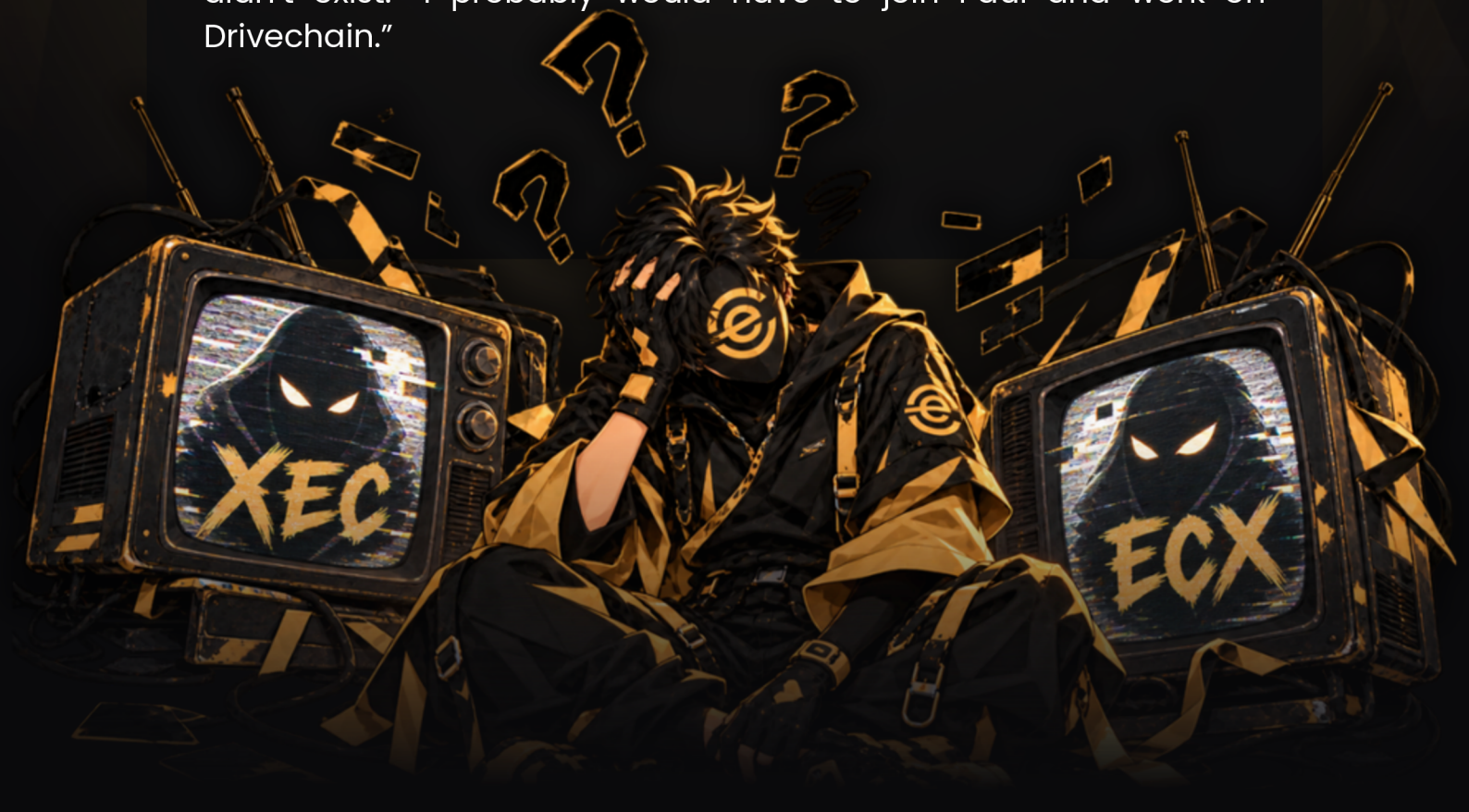
This is also why the staging matters. Alpha and Beta are the first time a Bitcoin fork has been rehearsed in public, on mainnet hashrate, with a kill switch. Whatever you think of Paul's opinions, this is a method other developers can borrow.

THE NAME PROBLEM

This magazine now covers two coins called **eCash**. Amaury Séchet renamed Bitcoin Cash ABC to **eCash in 2021**, and it trades as XEC. Paul owns the **ecash.com** domain and chose the ticker ECX. The name comes from Milton Friedman's 1999 remark that the missing piece of the internet was a reliable "**e-cash**," and from Satoshi's first draft of the whitepaper, which circulated as ecash.pdf. When I asked the Bitcoin Cash developers about it in S17 E26, Steve Thurmond called it "***a dick move***." Calin Culianu reduced the dispute to one line of Python: "ecash" == "ecash".

The collision is not only an insult. It is a phishing opportunity. Exchanges and wallet providers have already warned about fake "***claim your ECX***" sites. The rule is simple: *if you hold BTC in self-custody at the Mainnet snapshot, you already have ECX under the same keys*. Nobody needs your seed phrase. Anyone who asks for it is a thief.

There is one small, strange grace note. In the same S17 E19 conversation, I asked Amaury what he would work on if his eCash didn't exist. "I probably would have to join Paul and work on Drivechain."



THE RISK

REPLAY

Protection is opt-in. A Bitcoin transaction broadcast after the split may be valid on eCash too, unless you deliberately split your coins. Paul has said plainly that unprotected transactions will be replayed.



SECURITY

On the Alpha, the whole chain ran on about 0.001 percent of Bitcoin's hashrate. Any SHA-256 miner of moderate size could reorganize it. Sidechain escrows are only as safe as the honesty of a majority of that small hashrate.



EXCHANGES

If your BTC sits on an exchange at the snapshot, the exchange controls your ECX, and many exchanges have said they will not credit it. Japanese venues including Coincheck, GMO, SBI and Zaif took a cautious line during the Alpha.



WITHDRAWAL SPEED

Leaving a sidechain through the main peg takes months by design. Faster exits exist only through services that front you the money, which means trusting them.



CONCENTRATION

One company, one node implementation, one lead, and a genesis distribution that includes about 500,000 reassigned coins held by pre-launch investors.





WHO IS WHO

THE FORK

Paul Sztorc (“Truthcoin”)

Author of BIP-300 and BIP-301, founder and CEO of LayerTwo Labs, creator of Bitcoin Hivemind. The public face, the chief strategist and, often, his own sharpest critic’s best material.

CryptAxe

co-author of BIP-300 and BIP-301 and LayerTwo Labs co-founder, responsible for much of the code.

The eCash community

Whose running Alpha diaries on ecashblog.com are the best record of the rehearsal, and who are, understandably, not neutral.

Austin Alexander

LayerTwo Labs co-founder, formerly of Kraken.

LayerTree

The pool tag on the first Alpha block.



WHO IS WHO

THE CRITICS AND THE CONTEXT

Peter Todd

Whose 2023 analysis, paid for by LayerTwo Labs, remains the most discussed technical case against Drivechains.

Peter McCormack and Jameson Lopp

Who led the reaction to the Patoshi reassignment from opposite angles.

Luke Dashjr

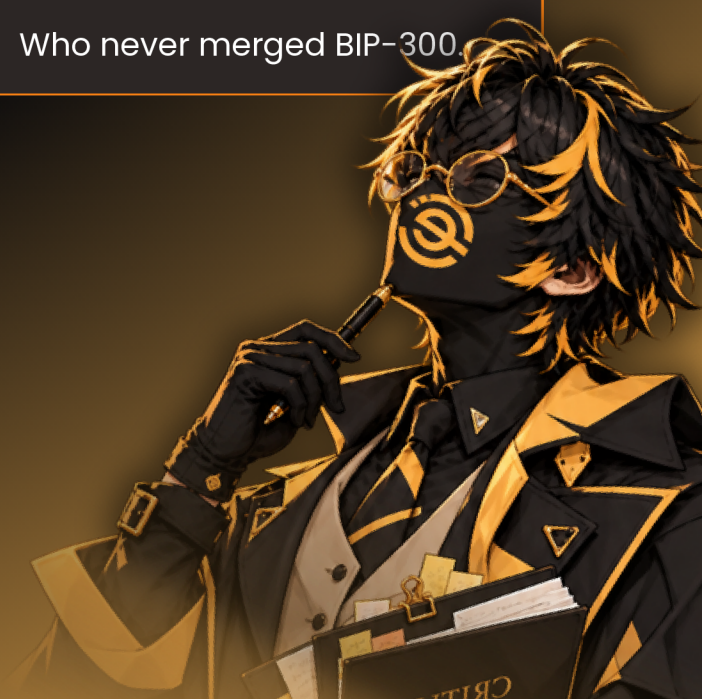
Who wrote a Core implementation of BIP-300, then led the rival fork of 2026.

Bitcoin Core maintainers

Who never merged BIP-300.

Amaury Séchet

Whose eCash (XEC) got to the name first.



WHAT ECASH HAS PROVED SO FAR

DRIVE CHAINS CAN RUN

Sidechains activated under proof of work and a withdrawal bundle was proposed on a live chain. What eleven years of argument could not settle was brought by a few weeks of rehearsal.

A FORK CAN BE REHEARSED

Alpha and Beta showed that a split can be tested on real hashrate before it becomes permanent.

DIFFICULTY IS THE FIRST ENEMY OF A MINORITY SHA-256 CHAIN

Rented hashrate arrived, pushed difficulty up, and stranded the network at a sixth of the hashrate it needed.

GENESIS CHOICES ARE FOREVER

Whatever eCash achieves, the reassigned Patoshi coins will be the first thing people mention.

HOLD YOUR FORKS

Keep your BTC in self-custody before block 973,728 and you will own ECX under the same keys, for free, whether or not you choose to touch it.



WILL IT FLIP BITCOIN

No. Paul doesn't claim it will either. He says he intends to keep his BTC, and he recommends you do the same. The main net eCash chain **does not exist yet**, the rehearsal ran on a thousandth of a percent of Bitcoin's hashrate, and the market for its coins is informal at best.

The better question is whether eCash will change Bitcoin. That depends on what happens after Halloween. If miners judge withdrawal bundles honestly, sidechains find users, and the chain survives its **first attempted theft**, Bitcoin will have for the first time real evidence about an upgrade it has argued over since 2015. If it fails, Bitcoin will have learned that cheaply too. Either way, after eleven years of being told his idea was dangerous, Paul will finally have data instead of opinions. I suspect he will say so, loudly, and in a way that annoys all skeptics. I also suspect that most of the time, **he will be right**.

SCORECARD INPUT

CRITERION	EVIDENCES
Technical ambition	Native BIP-300 and BIP-301; seven sidechains at launch; enforcer architecture; staged public rehearsal; continued merging of Bitcoin Core. The most ambitious feature set of any fork in this issue
Political radicalism	Fork after a decade of failed soft fork advocacy; reassignment of about 500,000 Patoshi-pattern coins to investors; opt-in replay protection; a name that collides with XEC; a founder who calls Core developers “corrupt”
Adoption	Pre-Mainnet; Alpha and Beta live; pECX traded informally; about 150,000 pECX burned; CoinMarketCap page with self-reported supply; major exchanges still cautious
Scalability claims vs measurement	Claims: global scale through Thunder and other sidechains. Measured: sidechains activated and a withdrawal bundle proposed on Alpha; no sustained throughput data yet
Decentralization	One company, one node implementation, one enforcer; SHA-256d lets any Bitcoin miner join; a concentrated investor allocation at genesis
Security model	Main-chain coins protected like Bitcoin’s; sidechain escrows protected by months-long majority miner voting; Alpha hashrate about 0.001 percent of Bitcoin’s
Long-run viability	Funded company since 2022; open repositories; public rehearsal culture; stated willingness to stand down if Bitcoin activates BIP-300. Counter-signals: Patoshi stigma, name confusion, thin security at launch
Speculative context	Upside: first real evidence for Drivechains, and a free airdrop to every self-custodied holder. Downside: replay losses, exchange non-support, a chain secured by a sliver of Bitcoin’s hashrate

SOURCES

SOURCES

ecash.com and its pages Why hard fork, What to expect, How to claim and Coin splitting; ecash-com/fast-facts integration guide; drivechain.info; BIP-300 and BIP-301; truthcoin.info, including "Blockstream's Big Mistake" (December 2025); ecashblog.com: "eCash ECX Hard Fork 101", "The eCash Alpha, Days 4 to 15", "Days 16 to 28", "Two Bitcoin Forks, Two Philosophies", and posts on Photon, Truthcoin and CoinShift; eCash Alpha explorer; mempool.space for fork-anchor hashes; Peter Todd, "Drivechains: A Detailed Analysis" (October 2023); CoinDesk on the LayerTwo Labs seed round (December 2022) and the Patoshi reassignment (April 2026); Bitcoin.com News on the announcement and the three-stage launch; CryptoSlate on the Alpha and exchange notices (August 2026); Because Bitcoin on the Patoshi debate; Bitrue on ECX scam warnings; Bitcoin Takeover Podcast S15 E68 and S17 E21 (Paul Sztorc), S17 E19 (Amaury Séchet), S17 E26 (Calin Culianu and Steve Thurmond).

ZCASH



THE PRIVACY MOON MATH BITCOIN WAS AFRAID TO INCLUDE



*In the spring of 2013, cryptographers at **Johns Hopkins University** created **Zerocoin** in order to make Bitcoin private. But the Bitcoin Core developers said no, and mostly for understandable reasons. Three years later the researchers **copied Bitcoin's code**, added the moon math themselves, and launched a separate chain. Ten years, two inflation bugs that most likely weren't exploited and one torched laptop later, Zcash is the most promising codebase fork of Bitcoin shipped so far, and the clearest record we have of what private money really costs.*

On a Sunday in May 2013, a **nervous PhD student** from Johns Hopkins walked onto the stage at the Bitcoin 2013 conference in San Jose. He apologised for being flustered: he had come straight from San Francisco, where his paper was about to be presented at the IEEE Symposium on Security and Privacy, one of the most selective venues in computer security. His name was Ian Miers. The paper was called Zerocoin, and he had about twenty minutes to tell a room full of early Bitcoiners that their favorite internet money was not as private as they believed.

He **opened with a joke about copying**. Making digital money that cannot be copied is nearly impossible, he said, and "*if you think about how easy it is for a fourteen-year-old kid to pirate the latest Justin Bieber album, and you consider that a twenty-dollar bill is probably worth considerably more than Justin Bieber, you have some idea about the scope of the problem*." Then he made his point: Bitcoin was not anonymous at all. It was pseudonymous, and pseudonyms leak. Two shops that see you under different names eventually notice that both names drive home to the same house. Data miners would link Bitcoin addresses the same way. Miers argued that this made Bitcoin worse than a bank account: "*At least in the case of the bank, it was the bank and whoever they told that knew your stuff. Your neighbors didn't, your family didn't, your co-workers didn't*." On Bitcoin, everyone would know.

His solution borrowed from **David Chaum**, the father of digital cash, and took away the bank. You would lock bitcoins into an "**opaque envelope**" recorded on the blockchain. Later you would prove, using a zero-knowledge proof, that you owned one of the envelopes in the pool, without revealing which one. He even had a way to explain it to children: you can prove you know where Waldo is by laying a huge sheet of paper with a small hole over the picture, so Waldo shows through the hole and nothing else does.

Miers was candid about where it might end up. "*How does this get adopted as part of Bitcoin? Okay, that's like the ideal, and not that likely*," he said. "*As part of some alternative currency, maybe. Or it becomes its own alternative currency, that actually has the claim to fame that it's really anonymous? I don't know*." He described himself as living in "*not quite an ivory tower. The roof leaks. It's not that tall, but close enough*."

Then the questions started. As Zooko Wilcox remembered it to me in **S16 E29 of the Bitcoin Takeover podcast**, Peter Todd stood up first, and his question "*was more of a statement*": "*The Bitcoin Core developers are not going to integrate a hard forking, experimental, inefficient protocol upgrade into Bitcoin right now*." The room microphones barely caught it, but Miers's reply survives on **the recording**: "*Yeah, that's a perfectly reasonable point.*" *Then someone asked about denominations. If everyone has to mint coins of the same fixed size, wouldn't a payment of an unusual amount stand out? "That would be trivially traceable*," Miers admitted.

Within those twenty minutes was nearly the whole history that follows: the cryptography, the doubts, Bitcoin's refusal, and an academic's correct guess that the idea would have to leave home to survive.

EXPLAINER: ZEROCOIN VERSUS ZEROCASH

Zerocoin proved that zero-knowledge privacy could work on a Bitcoin-style ledger. Zerocash made it practical.

	ZEROCOIN (MAY 2013)	ZEROCASH (MAY 2014)
Authors	Ian Miers, Christina Garman, Matthew Green, Aviel Rubin (Johns Hopkins)	The Zerocoin authors plus Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza
What it hides	Only the link between the coin you deposit and the coin you withdraw	Sender, recipient and amount
Amounts	Fixed denominations; an unusual amount gives you away	Any amount, and you can pay directly inside the shielded pool
Payments	Mix in, then spend as an ordinary visible bitcoin	Private payments from one person to another
Proof size	Tens of kilobytes (Miers quoted about 40 KB in San Jose)	288-byte proofs; transactions under 1 KB
Speed	About a second to mint; about half a second each to make and check a proof in the prototype	Verification in under 6 ms; making a proof took minutes on 2014 hardware
Setup	A trusted RSA modulus whose factors nobody may know	A circuit-specific trusted setup whose secret must be destroyed
Cryptography	Older, well-studied RSA assumptions	Newer pairing-based assumptions, which skeptics called “moon math”

EXPLAINER: ZEROCOIN VERSUS ZEROCASH

The jump came from zk-SNARKs, a newer kind of proof that the four extra authors had been making efficient, building on systems such as Pinocchio and BCTV14. Instead of special-purpose proofs for each step, Zerocash used one general-purpose proof that a whole hidden transaction followed the rules. “Zerocash sort of threw SNARKs at the problem,” Sean Bowe told me in S16 E51. The trade-off was that Zerocash needed a trusted setup and newer cryptographic assumptions, and those were exactly the parts Bitcoin’s developers trusted least.

Zooko was in San Jose that weekend too. A two-person startup called Coinbase offered him a job as its security chief at a folding table, and he turned it down. He did not see Miers’s talk, but he says the Hopkins group and the four SNARK researchers met there; Ben-Sasson gave his own talk on succinct proofs at the same conference. In Zooko’s words, “the four scientists met the three scientists and joined forces and became the seven scientists.”



SATOSHI'S UNFINISHED WISH

The idea was older than all of them. In August 2010, someone on Bitcointalk suggested that zero-knowledge proofs might help Bitcoin. **Satoshi replied** that it was hard to see how they would apply, but added that if a solution could be found, a much better, easier, more convenient implementation of Bitcoin would be possible. "*And then four months after he posted that, he disappeared from the internet forever," Zooko told me.* "And then three years after that, these scientists, who didn't include me, found a solution."

Zooko had been waiting longer than most. In the 1990s he worked at David Chaum's DigiCash in Amsterdam, chasing a decentralized version of Chaum's cash in his spare time. "*I was trying to invent Bitcoin for like 15 years unsuccessfully before Satoshi invented Bitcoin,*" he said. When Zerocoin appeared, "my eyes lit up, and I said to myself, this is the first thing that could actually work." He saw Bitcoin's transparency as a deep design flaw: "*You can't use Bitcoin for anything without unwillingly disclosing your current assets and all of your past transactions and all of your future transactions.*" He also liked the name: "*the word zero in the name Zerocoin is named after zero-knowledge proofs, which are named after leaking no information about you.*"

In early 2014, Matthew Green presented **Zerocash** at the Real World Crypto conference. Zooko was first at the microphone. "*This is great. This is awesome. Best thing ever," he said. "But what about that trusted setup thing?*" Green's answer, a recorded ceremony and a destroyed computer, did not satisfy him, and he kept pressing. A few weeks later Green called and asked him to help turn Zerocash into a real currency. When the company appeared on AngelList in 2015, **Wired reported** its pitch in one line: "*Bitcoin is HTTP for money. We are HTTPS.*"

WERE BITCOIN DEVELOPERS RIGHT?

On the narrow question, yes, and the decade since has proven it.

If Bitcoin had soft-forked Zerocoin in 2013, it would have inherited a protocol in which researchers **found a cryptographic flaw in April 2018** that let an attacker destroy honest users' coins, create coins from nothing, or steal them. If it had adopted Zerocash in 2014, it would have inherited **the flaw in BCTV14** found in March 2018, which made counterfeiting possible for anyone who noticed some extra numbers in the setup transcript. It would also have been exposed to the 2026 Orchard bug, which sat undetected for four years. And it would have had to run a trusted setup and ask every Bitcoiner to believe the secret had been destroyed.

Bitcoin has had inflation bugs of its own, in 2010 and *2018*, but in both cases anyone could see and count the damage. In a shielded pool, a counterfeit coin looks like every other coin. Peter Todd made the point again in 2026: "The privacy of Zcash makes inflation exploits far more dangerous."

Even Zcash's builders concede the point. "Bitcoin Core probably [was] right," Josh Swihart said in *S15 E62*. "The cryptography was too novel at the time." Sean Bowe never expected Bitcoin to say yes: "If you ever interacted with the Bitcoin developers back then, they were absolutely not going to ever add something like that."

WHY SOMEONE STILL HAD TO TRY

Bitcoin's caution was right for BTC. But someone had to run the experiment, because a paper cannot tell you two things: whether the technology survives contact with real money, and whether anybody wants it.

The first question is about refinement. Ideas get better when they are shipped. Bowe describes the trap Maxwell was pointing at: a conservative chain waits for the perfect version, and "*a new paper's going to come out and say, oh, I have a way to do it ten times faster and with better trust assumptions.*" Zcash took the opposite view. "*We're willing to take what we have that we know works and change the protocol completely to implement it, as fast as we can safely*," he said. Nearly every improvement he made came from fixing real problems in a live system: proofs fast enough for phones, setups with 87 participants instead of six, and finally Halo, which needed no setup at all. "*You can be clever and everyone can praise you for your papers, and that's great for your resume, but it doesn't actually do anything*," he told me. "**Shipping is crucial**."

The second question is about demand. A testnet gives you no answer, because nobody's money is at stake. Zcash spent years as a technology everyone admired and almost nobody used. Then wallets made shielding the default, and the numbers changed. By late September 2026, **according to CoinDesk**, about 4.9 million ZEC, roughly 29 percent of issued coins, sat in shielded pools, and one week recorded about 63,000 shielded transactions, the busiest since 2022. Those numbers show demand that no academic paper could have measured.

Bitcoin itself learned something too. In **S16 E51** I told Sean that when I asked Peter Todd to name altcoins he considered legitimate, he named Litecoin, Monero and Zcash. The technology was "**actually interesting**," he said, "*and they have made great progress*." In September 2026, researchers at [alloc] init published "**Shielded Bitcoin**," a proposal for Zcash-style encrypted payments on Bitcoin that needs no consensus change. The idea Bitcoin declined in 2013 is being proposed again, partly because Zcash shipped it first.

THE BOX UNDER MY BED



For me, this story became personal through a cardboard box sealed with duct tape.

In 2021, at the height of the NFT craze, I bought a collectible from **Peter Todd** for $1111 in bitcoin: the remains of the laptop he used in October 2016 to help create **Zcash's first shielded pool**. It is one of **six computers in the world** that took part in the ceremony that launched Sprout. As far as I know, it is the only one sold to a collector. The processor is gone; Todd destroyed it on purpose. What remains is a cooling fan, a heat sink still smeared with thermal paste, a gutted hard drive and a set of Verbatim DVDs. One envelope reads "**burnt compute node remains**," sealed by Todd on 26 October 2016. Another is labelled "**final MPC compute node, test burn #1, #2, Tails**," sealed "**at midnight on Monday, October 24, 2016.**" He drew his pen across every seal, so that opening one would break the line. "**On one hand amateurish, but rigorous,**" I said on air while I cut it open with a pen. I kept it sealed under my bed for years, waiting for someone who could explain it properly. In **S16 E29** I opened it on camera, with Zooko there to explain it.

The DVDs are the important part. Under Zooko's rules, each ceremony computer had its **Wi-Fi and Bluetooth removed** and was never plugged into a network. The only way data could get in or out was a disc burner. "**The six discs you have there**," Zooko told me, "**are the only six messages that emitted from that compute node between the time it was random-purchased at the store and the time it was destroyed.**" They let anyone check that the parameters Zcash nodes used were the ones the six participants actually produced.

For two years, those discs were dangerous. In March 2018, the cryptographer Ariel Gabizon found that **the BCTV14 proof system** behind Sprout had told the ceremony to generate some extra elements it never needed. Those elements ended up in the ceremony transcript, which was simply all six participants' DVDs joined together, and they were enough to forge proofs. Anyone who had the transcript, and understood what was in it, could have created counterfeit Sprout coins. According to Sean Bowe, one of the discs in my box, probably D or F, contains that data. From Zcash's launch on 28 October 2016 until the **Sapling upgrade** on 28 October 2018, information that could break the money supply existed on optical discs scattered around the world, including the ones that later sat under my bed.

Eran Tromer had warned about exactly this. In 2016 he argued against publishing the transcript at all. "I was like, ah, Eran, you worry too much," Zooko said. "I was totally wrong and Eran was totally right." Once the flaw was found, the team deleted the public transcript. Bowe encrypted what was probably the last complete copy and handed the key to Zooko, so that reaching it would take both of them. Then a small group fixed the problem in secret for eleven months. The Sapling upgrade moved Sprout onto a different proof system with new parameters, so the old elements could no longer forge anything. ECC **disclosed the flaw in February 2019**. Afterwards, Bowe had to rebuild the transcript as a historical record from the participants' discs. Todd declined to help. A videographer who had filmed the ceremony turned out to have downloaded the missing discs, some of them corrupted, and it was just enough. Since 2018, my DVDs have been a museum piece rather than a weapon.

There is no evidence the flaw was ever exploited. A rule Zcash had in place from launch, the turnstile (later formalised in **ZIP 209**), sets a hard limit: coins can leave a shielded pool only through the transparent side, so each pool's balance is public, and no pool can pay out more than it ever took in. New deposits into Sprout were disabled by **ZIP 211** in the **Canopy upgrade** in 2020, and the pool has since dwindled to about 25,600 ZEC. "There's no way it was exploited, I think," Bowe said, "and if it was, there's a cap on the impact."

That box is also where this year's other project begins. I am making a documentary, Zcash: From Zidelined to Zillions, built from footage of my **Bitcoin Takeover interviews** with Zooko, Sean Bowe, Josh Swihart, Kris Nuttycombe and others, including the unboxing. It will be released around Zcash's tenth anniversary, on 28 October 2026.



VITAL STATISTICS

Market data from 17 September 2026 (CoinMarketCap, CoinGecko); shielded data from 25 September 2026.

FIELD	VALUE
Ticker	ZEC
Category	Codebase fork of Bitcoin Core with its own genesis block; no shared history and no airdrop to Bitcoin holders
Origin	Zerocoin (May 2013) and Zerocash (May 2014) papers; Johns Hopkins, MIT, Technion and Tel Aviv University
Genesis	28 October 2016; the tenth anniversary is 28 October 2026
Proof of Work	Equihash (200, 9); ASIC-mined since 2018. ViaBTC held about 73 percent of hashrate in October 2025
Blocks	75 seconds (150 seconds before Blossom, December 2019); 2 MB limit
Supply	21 million cap, Bitcoin-style halvings; about 16.9 million issued (protocol specification)
Shielded pools	Sprout 2016 (about 25,600 ZEC, closed to deposits), Sapling 2018, Orchard 2022 (withdrawal-only since July 2026), Ironwood 2026
Shielded supply	About 4.9 million ZEC, roughly 29 percent of issued coins; about 63,000 shielded transactions in the week to 25 September (CoinDesk)
Trusted setups	Six participants (Sprout, 2016); 87 contributions (Powers of Tau, 2018); none since Orchard (Halo 2, 2022)
Counterfeiting bugs	Two found and fixed (BCTV14 in 2018, Orchard in 2026); no known exploitation; a turnstile on every pool
Proof system today	Halo 2, with Ironwood's balance integrity machine-checked in more than 2,700 Lean theorems
Upgrade pace	Roughly yearly network upgrades; about 18 months from idea to mainnet for past pools, according to Sean Bowe
Latest upgrade	NU6.3 Ironwood, block 3,428,143, 28 July 2026
Development funding	20 percent of block subsidy: 8 percent to Zcash Community Grants, 12 percent to a coinholder-controlled fund (ZIP index)
Nodes	Zebra (Zcash Foundation) and Zakura; zcashd retired in July 2026
Market	About $22.7 billion market cap (about 1.48 percent of Bitcoin's), CoinMarketCap rank 9; price about $1340

THE CEREMONY

The zk-SNARKs of 2016 needed public parameters, and making them produced a secret by-product. "I decided to call the secret the toxic waste," Zooko said. Anyone who kept it could print unlimited shielded ZEC without detection. It could not reveal anyone's transactions; it could only counterfeit. The fix was a **multi-party computation**. "*There's these six different chemicals, and if you mix all of them together in the same room, they turn into this horrible toxic waste,*" Zooko explained. "*So what we're going to do is keep the six precursors separate from each other and not allow them to mix.*" If even one participant destroyed their share honestly, the waste could never be assembled.

Why six? "*The protocol took hours, and if we had more people it would take more hours, and we couldn't fit it into one weekend.*" Zooko recruited eight or nine, then told all but six at the last moment that they had been decoys, there to distract hackers. He gave three of the six pseudonyms. Every participant had to buy a new computer in person and never let it out of sight, a practice Edward Snowden taught him called "**random purchase.**" When Zooko visited Julian Assange in the Ecuadorian embassy, Assange's advice was to "*double down on the air gapping part.*" Zooko's own station was filmed around the clock by cameras bought used in Denver, because "you couldn't buy a camera that didn't have Wi-Fi in 2016." The journalist Morgen Peck watched on site and wrote it up for **IEEE Spectrum**; her reporting also became **Radiolab's "The Ceremony"**.

The six stations over the weekend of 22 and 23 October 2016 were:

- **Zooko Wilcox**, in Colorado.
- **Peter Van Valkenburgh** of Coin Center, who cut his RAM apart with tin snips.
- **Derek Hinch** of NCC Group.
- **Andrew Miller**.
- "**John Dobbertin**," revealed in 2022 as Edward Snowden.
- **Peter Todd**, who ran his computation in a car driving across Canada and then burned the machine with a propane torch. "It was my goal to outdo every other station in Canadian cypherpunk glory," he wrote in "Cypherpunk Desert Bus."

Sean Bowe, then 23, coordinated the whole thing and, at one point, pasted a 4chan meme into the group chat by mistake: "I found out it was Edward Snowden much later. I was like, ah crap, that's embarrassing."

Todd later disowned his part, writing that the setup should not be "*called a multiparty computation, which makes my involvement pointless.*" His worry was the software: "*There are lots of ways someone could have surreptitiously changed it.*" *Bowe's reading: "It lent legitimacy to Zcash that he didn't want to lend."*

THREE POOLS AND THE END OF THE CEREMONY

Sprout (2016) was the proof of concept. “You couldn’t run it on a mobile device,” Zooko admitted. Making a transaction “used up all your RAM and heated up your CPU for like 40 seconds.”

Sapling (2018)

Made shielded payments work on phones, with parameters from the 87-contribution Powers of Tau ceremony that Bowe designed.

Orchard (2022)

Ended the ceremony entirely. Bowe, working with Jack Grigg and Daira-Emma Hopwood, found **Halo** in 2019, the first practical way to build recursive proofs without a trusted setup. Bowe says the removal was almost a side effect: “I would have actually been totally happy with Halo at first if it didn’t solve the trusted setup problem.” **Halo 2** became Orchard’s foundation. Six years after Peter Todd’s torch, nobody had to destroy anything.

HOW ZCASH DIFFERS FROM BITCOIN

	BITCOIN	ZCASH
Relationship	Original chain	Fork of Bitcoin Core's code; separate genesis
Privacy	Transparent ledger	Optional shielded pools that hide sender, recipient and amount
Supply audit	Add up the UTXO set	Transparent supply plus a turnstile on each pool
Proof of work	SHA-256d	Equihash
Blocks	About 10 minutes	75 seconds, 2 MB
Upgrades	Rare soft forks	Scheduled network upgrades, roughly yearly
Funding	Donations and companies	20 percent of block subsidy
Nodes	Bitcoin Core, Libbitcoin	Zebra, Zakura

WHO PAYS FOR ZCASH

For the first four years, 20 percent of every block subsidy went to founders, investors, staff and the Zcash Foundation. This was the Founders' Reward, about 10 percent of the eventual supply. Critics called it a premine. Zooko calls it the reason Zcash kept improving: "We could have stopped in 2016, but that would have been a pretty meager contribution to mankind compared to what we've got today." The Dev Fund that followed (**ZIP 1014**) split the 20 percent among the Electric Coin Company (ECC), the Zcash Foundation and a grants programme. At the **2024 halving**, Josh Swihart, who had **taken over as ECC's chief executive** in December 2023, refused to renew ECC's share. "I didn't think for a public good it was appropriate for any organization's addresses to be baked into the chain, nor to be guaranteed funding," he said in **S17 E28**. Today 8 percent goes to Zcash Community Grants and 12 percent to a lockbox that coinholders have controlled since **NU6.1** in November 2025.

In January 2026, after a dispute with the board of the Bootstrap Project, ECC's nonprofit parent, the entire ECC team left. "Within a week" they had formed the Zcash Open Development Lab (ZODL), a for-profit that earns 50 basis points on in-wallet swaps. ECC is being wound down. **Shielded Labs**, where Zooko now leads product, is developing Crosslink, a hybrid of proof of stake and proof of work, and the **Network Sustainability Mechanism**.

THE CRITICS

Riccardo Spagni, the former Monero lead, told me in **S17 E8** that he considers Zcash a “scam” in the same sense as Ethereum. He meant a project built by “technically competent people who make stupid decisions when it comes to architecture or design… in full knowledge.” His core argument is that privacy should be on by default: “You shouldn’t wait for scaremongering to happen to turn the switch on. The switch should be on from the get.” On the funding: “If it was just researchers creating a thing that they hoped would become a model for Bitcoin, why did they raise money?” Zcash’s builders reply that a shielded transaction hides among the entire history of its pool, while a Monero ring signature hides among a handful of decoys. Zooko adds that “you cannot add privacy to money in flight, you can only add privacy to money at rest.”



THE ORCHARD CRISIS OF 2026

On 29 May 2026, Taylor Hornby, a security researcher working with Shielded Labs, reported a soundness bug in Orchard's circuit. It had been live since 2022 and could have allowed coins to be minted inside the pool. A soft fork paused Orchard, and NU6.2 restored it on 3 June. ZEC roughly halved in price, and holders withdrew about 800,000 ZEC. Swihart defended disclosing everything in S17 E28: "It eroded some trust in the shielded pool, because people can't see inside. But it increased the trust of the teams."



EXPLAINER: IRONWOOD AND TACHYON

Ironwood (NU6.3, 28 July 2026) moved shielded funds to a corrected pool and made the old Orchard pool withdrawal-only. That turns the migration into an audit: every coin leaving Orchard passes the turnstile. It also comes with a **machine-checked proof in more than 2,700 Lean theorems** that the pool cannot create undetectable counterfeit coins. "Zcash's new formal verification efforts eliminate undetectable counterfeiting bugs from the new Ironwood pool," Bowe wrote. It also adds quantum-recoverable notes.

Tachyon is Bowe's plan to scale private money in three parts:

BOWE'S PLAN

SHIELDED AGGREGATION

A block's shielded transactions are folded into a single recursive proof.

OBLIVIOUS SYNCHRONIZATION

An outside service tracks the chain for your wallet without learning anything about it.

NO IN-BAND SECRETS

Payment details travel directly between sender and recipient instead of being stored on chain.

Validators could then delete old spending records instead of keeping them forever. "If privacy can't scale now, then nothing can," Bowe said in **S16 E51**. "So it's math, and it's also vibes." Most of Tachyon is not live yet.



WHO IS WHO

THE AUTHORS



Ian Miers, Christina Garman, Matthew Green and Aviel Rubin

Who designed Zerocoin at Johns Hopkins.



Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer and Madars Virza

Who joined them to create Zerocash.

THE CEREMONY



Peter Todd, Edward Snowden, Peter Van Valkenburgh, Derek Hinch, Andrew Miller and Zooko Wilcox

With **Morgen** Peck as witness.

THE SKEPTICS



Greg Maxwell, Peter Todd and Riccardo Spagni.

THE WATCHER



Hal Finney

WHO IS WHO

THE BUILDERS



Zooko Wilcox-O'Hearn

Zcash's founder.



Nate Wilcox

His brother and business partner.



Ariel Gabizon

Who found the 2018 flaw.



Josh Swihart

Head of ZODL.



Kris Nuttycombe

Wallet and SDK engineer.



Taylor Hornby

Who found the 2026 Orchard bug.



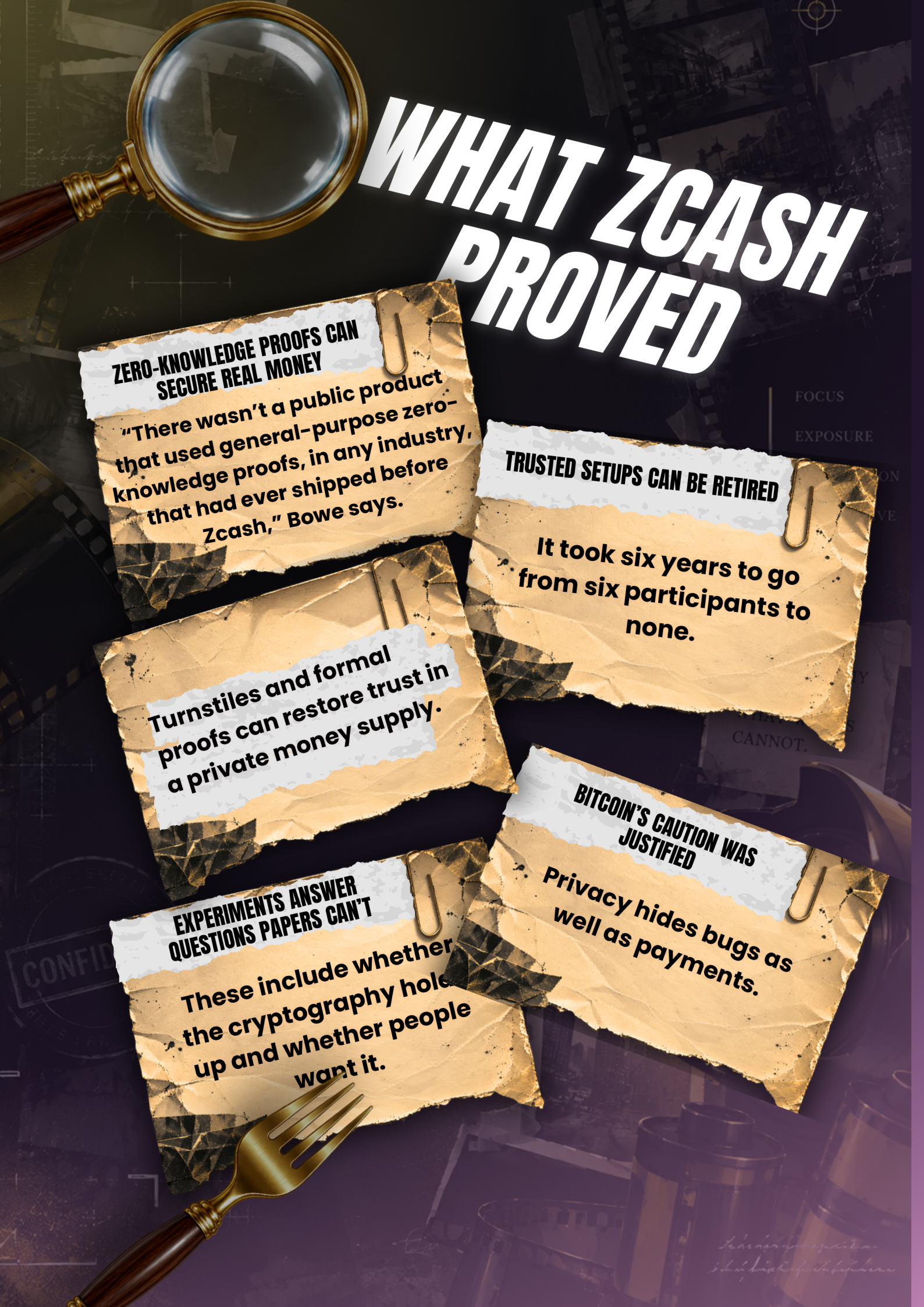
Sean Bowe

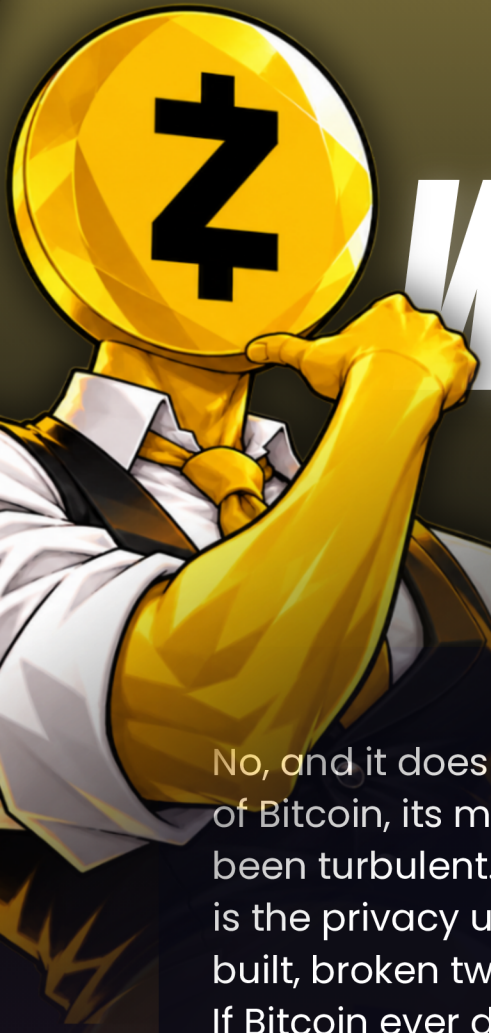
Who coordinated the ceremony and leads Halo and Tachyon work.



Daira-Emma Hopwood and Jack Grigg

Protocol designers.


WHAT ZCASH PROVED
ZERO-KNOWLEDGE PROOFS CAN SECURE REAL MONEY
"There wasn't a public product that used general-purpose zero-knowledge proofs, in any industry, that had ever shipped before Zcash," Bowe says.
TRUSTED SETUPS CAN BE RETIRED
It took six years to go from six participants to none.
Turnstiles and formal proofs can restore trust in a private money supply.
BITCOIN'S CAUTION WAS JUSTIFIED
Privacy hides bugs as well as payments.
EXPERIMENTS ANSWER QUESTIONS PAPERS CAN'T
These include whether the cryptography hol up and whether people want it.



WILL IT FLIP BITCOIN?

No, and it does not really try. Zcash is worth about 1.5 percent of Bitcoin, its mining is less distributed, and its governance has been turbulent. Its claim is narrower and harder to dismiss: it is the privacy upgrade Bitcoin was offered in 2013, actually built, broken twice, and rebuilt around a mathematical proof. If Bitcoin ever decides it wants shielded payments, it will benefit from more than a decade of research data and hard fork in the field of zero knowledge proofs. So adding it today is much safer than adding it in 2014 because the understanding of the technology is better and there are more experts around the world who can verify the code. Unfortunately, it appears that Bitcoin is stuck from a technical evolution point of view... which lends much more legitimacy to projects like Zcash and enables them to flourish in the markets where BTC is no longer competitive. So there is room for a battle for users and network effects, but it seems unlikely that ZEC will flip BTC any time soon.



SCORECARD INPUT

CRITERION	EVIDENCES
Technical ambition	First production zk-SNARK currency; Halo 2; formally verified Ironwood; Tachyon
Political radicalism	Challenges Bitcoin's transparency; permanent development funding; the 2026 ECC rupture
Adoption	Rank 9; about 29 percent of supply shielded; exchange friction
Scalability claims vs measurement	75-second blocks live; Tachyon gains are design targets
Decentralization	Several organizations, two node implementations, concentrated ASIC pools
Security model	Equihash, turnstiles, two fixed bugs without known exploitation, Ironwood proof
Long-run viability	Ten years of shipping; chain-funded development; organizational churn
Speculative context	Upside: private payments, quantum-ready design. Downside: regulation, complex cryptography, governance conflict

SOURCES

BITCOIN TAKEOVER PODCAST

- **S16 E29: Zooko on Ecash, Bitcoin & Zcash**
- **S16 E51: Sean Bowe on Bitcoin, Zcash, Scaling & Privacy**
- S15 E62 (Josh Swihart and Kris Nuttycombe), S17 E8 (Riccardo Spagni), S17 E26 (Bitcoin Cash developers) and S17 E28 (Josh Swihart), all in the **podcast archive**
- **Bitcoin Forks, Described by Dorks**, the timestamped quote archive

PAPERS

- Miers, Garman, Green and Rubin, "**Zerocoin: Anonymous Distributed E-Cash from Bitcoin**", IEEE S&P 2013
- Ben-Sasson et al., "**Zerocash: Decentralized Anonymous Payments from Bitcoin**", IEEE S&P 2014
- **Pinocchio** and **BCTV14**
- Gabizon, "**On the security of the BCTV Pinocchio zk-SNARK variant**"
- Bowe, Grigg and Hopwood, "**Recursive Proof Composition without a Trusted Setup**" (**Halo**)
- Biryukov and Khovratovich, "**Equihash**"
- Back et al., "**Enabling Blockchain Innovations with Pegged Sidechains**"

SOURCES

PRIMARY POSTS, TALKS AND DOCUMENTS

- Ian Miers, "**Zerocoin: A New Anonymous eCash Extension for Bitcoin**", Bitcoin 2013, San Jose
- **Zerocoin Project talks and press**
- Greg Maxwell, "**CoinJoin: Bitcoin privacy for the real world**", August 2013
- **Satoshi Nakamoto on zero-knowledge proofs**, August 2010
- Hal Finney, "**Looking at ways to add more anonymity to bitcoin**" and "**Bitcoin and Me**"
- **Bitcoin Magazine Issue #12**, July 2013
- Peter Todd, "**Cypherpunk Desert Bus**"
- **Zcash parameter generation**
- ECC, "**Zcash Counterfeiting Vulnerability Successfully Remediated**", February 2019
- **Zcash protocol specification**, **ZIP index**, **ZIP 209**, **ZIP 211** and **ZIP 1014**
- Upgrade pages: **Sapling**, **Blossom**, **Canopy**, **NU5** and **NU6.1**
- ECC on **the 2023 leadership change** and **the 2024 halving**
- Project Tachyon, "**Ironwood verification complete**"
- Sean Bowe, "**Tachyon: Scaling Zcash with Oblivious Synchronization**"
- **Halo 2 book**, **Zebra** and **Shielded Labs NSM**
- Bitcoin's own bugs: the **2010 value overflow incident** and **CVE-2018-17144**

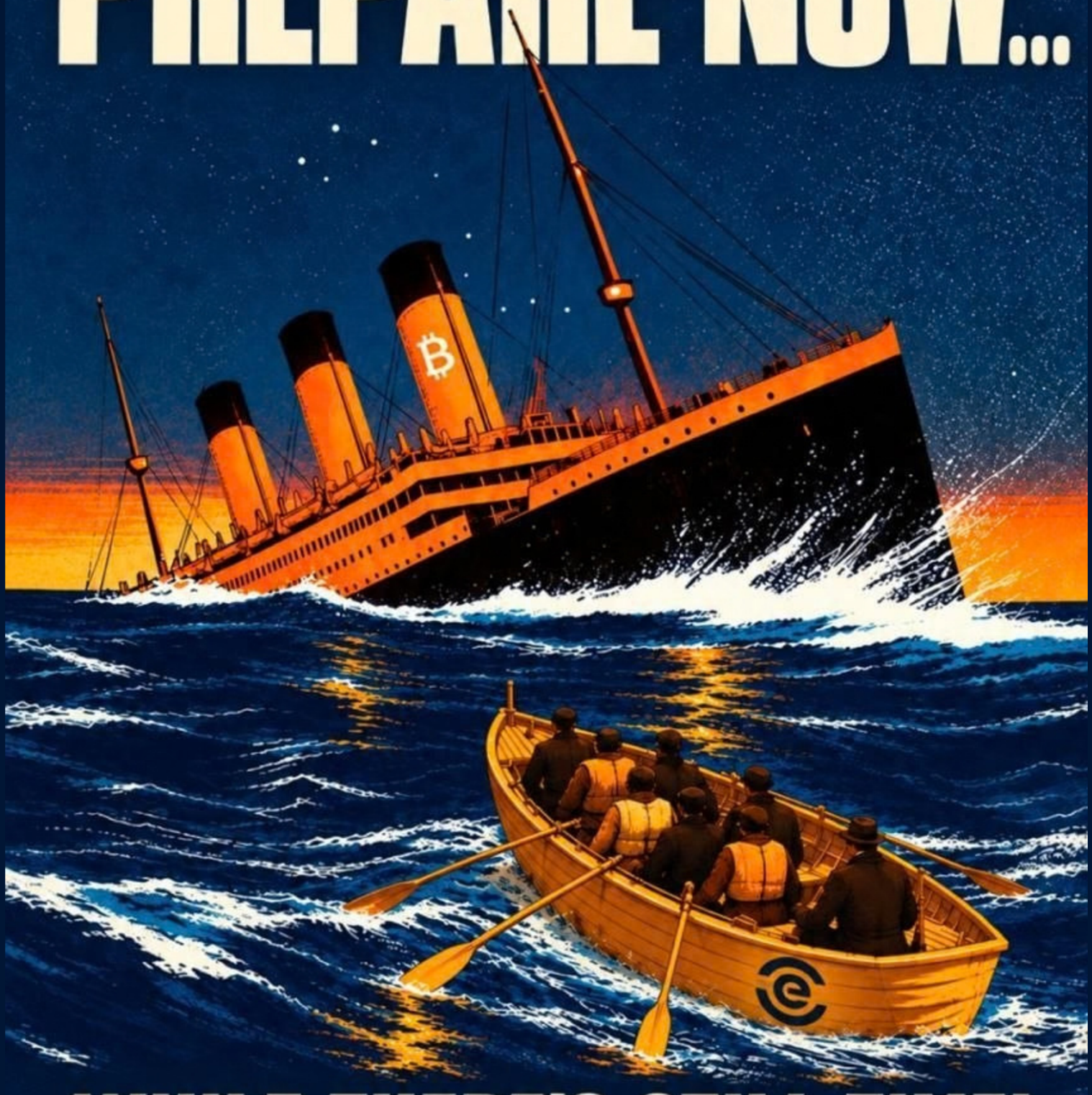
BTCTKVR PODCAST

SEASON 17



"SCAN ME, I WON'T BITE!"

PREPARE NOW...



WHILE THERE'S STILL TIME!

eCash.com

NEW BITCOIN HARDFORK • L2 DRIVECHAINS

OCT 31 2026 MAINNET TARGET

DONATIONS SO FAR



JEREMY

The Bitcoin Cash Podcast

FOR AS LITTLE AS

$50

YOU CAN ADD YOUR NAME HERE TOO!