

Why Hard Fork

Why are we doing this project?

A New Hard Fork of Bitcoin

Iron sharpens iron
- Proverbs 27:17

The time has come for the Bitcoin Community to revisit the “hard fork”.

The upside is enormous: global scalability, privacy, competition, rapid improvement and adoption. In fact, it may be a matter of life or death, for Bitcoin.

The downside is small: some drama, plus every Bitcoiner gets some free money.

1. An Altcoin? You are leaving Bitcoin?!

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, to maximize their revenues (and the utility of the coin). Bitcoin culture has [many entrenched errors](#), and is probably unfixable at this point.

2. Errors? Isn't Bitcoin perfect? Nothing can stop Bitcoin!

I hope Bitcoin succeeds. I plan to hold my BTC – and so should you.

If Bitcoin is unstoppable, then eCash is nothing to worry about. Just stop reading now.

Alternatively, though – if I am correct [that Bitcoin is *not* perfect], then it would be wise to prepare. What's our backup plan? It is eCash.

Even if Bitcoin is perfect now – will it remain perfect? New ideas are invented all the time! (After all, there was a time before you had ever heard of Bitcoin.) And there's no limit to *how large* a mistake the Bitcoin Community might someday make.

Ironically, the “Bitcoin is perfect” belief, is likely to be what finally kills Bitcoin. Success often leads to complacency, and failure. The Titanic was hailed as “unsinkable” – it sank on its first voyage. The book “Innovator’s Dilemma” details the history of bankruptcies in tech – it is usually easier to start a new company, vs fix an old one.

3. I don’t like what you are doing, becau–

Let me stop you right there.

You are getting free eCash... so: sell it! Use it to get *more BTC*. Do that, instead of complaining.

You can think of this project as “free number-go-up” on your BTC. You’re welcome!

4. You really think a new coin can defeat Bitcoin?

Yes. It is at least 5% likely.

Even at such a “low” chance of success, eCash is still worth trying. The Bitcoin project is too important, to let today’s idiots screw it up.

We need *competition* – a red team / blue team style competition. That is what is healthy for BTC.

5. Why is a hard fork necessary? Please describe each technical change you are making.

The hard fork is NOT needed for any technical reason.

It is not the BTC code that is broken – it is the BTC community. We need to bet *against* that community. So – we need a new coin.

Our L1 is a clone of Bitcoin Core, with these changes:

1. **Difficulty Reset** – A one-time “special difficulty adjustment”, down to the *minimum* difficulty, on the fork date.
2. **Satoshi Half-Airdrop** – We give *half*, of Satoshi’s “patoshi” coins (about 550k of 1.1 M) – to our investors and supporters.
3. **Txn Replay Control** – We allow our txns to have an optional “extra byte” – this intentionally mangles the TxID, allowing users to opt in/out of “transaction replay”.
4. **The Name** – Superficial changes (the name, the “network magic”, seed node IPs, etc).

Furthermore, we plan to immediately adopt two *soft forks* (that BTC is unwilling to adopt):

1. Reduce blocksize by 10x – ie, from 4 MB to 400 kb.
2. Activate BIPs 300/301.

Both of these can be done via “CUSF” – (ie, without changing any lines of code).

We will intentionally keep our L1 codebase identical to Bitcoin Core for as long as possible – ideally forever. By doing so, we automatically gain access to CVE fixes, and new Core features (without doing any work). We do not want to compete with Core, on L1.

6. Aha! You are taking Satoshi’s coins! That is why you are doing this! Thief!!

Well, again:

1. We’d prefer not to do this, at all.
2. If BTC activates BIPs 300/301, we will abandon this project (unless the eCash marketcap is higher than BTC, at that time).

And, the facts are:

1. We are “stealing” zero of Satoshi’s BTC. (We do not have the power to take BTC.)
2. In fact, we are *giving* Satoshi free eCash.
3. Admittedly, in a hypothetical future scenario where eCash replaces BTC, then Satoshi would have fewer coins – but, in that world, the eCash marketcap almost certainly exceeds today’s BTC marketcap, by more than 2x. So, the *value* of Satoshi’s holdings, will have gone *up* (from where it is today), due to our actions.
4. In fact, in that scenario, it could be argued that we *rescued* Satoshi’s net worth, from \$0.
5. Our project contains a zk-snark privacy L2 – this might be *the only* safe way for Satoshi to access his coins.

On top of that:

1. Innovators are certainly entitled, to make some return on their risk (at the expense of their haters).
2. It is *immoral* for Bip300-supporters and Bip300-haters to be treated equally, in this case.

And:

1. We intentionally want to split the community, and drive away the overly-conservative faction. (Those are the “bad guys” who are killing BTC.)
2. We want new people: open-minded, entrepreneurial, risk-taking, contrarians. We want to

shake things up, and prioritize the new over the old.

Finally:

1. *Lack of competition* is killing the BTC project. It is an existential risk, that warrants bold action.
2. If you don't like it – then *sell*. (See answer #3.)

7. Doesn't the failure of Bitcoin Cash (BCH), prove that hard forks always fail?

Bitcoin Cash launched at a [sky-high price \(of 15% BTC\)](#). It “flipped” Ethereum for one day, temporarily becoming the #1 Altcoin.

If our fork repeated that 15% performance, it would launch at \$15,000/coin and linger in that area for about 6 months.

BCH had many strengths: the support of large investors (such as Roger Ver), key resources (such as the “bitcoin.com” domain), and a pre-assembled community of largeblockers.

But those are easy to recreate. We have our own “.com”, we have our own large investors, and –thanks to the hard fork– we replicate the #1 crypto community in the world (the Bitcoin community). The crypto community has already blazed the trail – everything from community management, to forum software, to regulatory clarity.

More importantly, Bitcoin Cash suffered from [a long list of fundamental problems](#). Each of these was debilitating – and each is also easily avoided. We will avoid all these problems.

What if we share the exact fate of BCH? Today, BCH is worth over *ten billion dollars* (over 500 \$/coin). Not bad... for a “failure”!

8. How do you plan to dethrone BTC?

It will be difficult.

Here are the general principles:

1. Do not compete with BTC where it is strong.
 - Keep L1 identical.
 - Keep the fixed supply, 21 million, proof of work, etc.
 - Let BTC do the “leg work”, of educating the masses.
 - Keep all wallet software, block-explorers, etc identical.

- This lowers switching costs, maintenance costs, and eliminates the need for cumbersome explanations.
2. Use tech to guarantee liquidity.
 - Use cryptographic swaps to trade eCash for BTC.
 - BTC is now an on-ramp for eCash! Therefore, any BTC liquidity, also becomes eCash liquidity.
 - Exchanges (in practice) must list eCash. (No need to pay exorbitant listing fees.)
 - This also flips the “all privacy coins will be de-listed” narrative – since you can’t delist eCash (a coin with a private L2) without de-listing BTC.
 3. Focus on what BTC can’t do:
 - Tech innovation / tech competition – (currently roadblocked by Core / prestige economy).
 - Privacy – (currently roadblocked by Saylor / corporate interests).
 - Mining Revenue – (currently roadblocked by non-mined L2s; superstitions about mining).
 - Fun – (currently roadblocked by Bitcoin twitter).
 - Specific use-cases (BitNames, BitAssets, Coin-Swaps, Prediction Markets) – (currently roadblocked by maxi culture).
 4. Focus on users.
 - Define users as: those who pay transaction fees to miners.
 - In contrast, non-users are: developers, miners, investors, and media personalities.
 - In the long run, users win. Non-users are parasites who must be kept at bay (when necessary).
 5. Sabotage BTC, by promoting “degrowth” policies such as...
 - Complacency narratives: ossification, “Bitcoin has already won”, “Don’t break bitcoin”.
 - Failed L2 concepts, such as Lightning.
 - Distractions, such as Covenants.
 - Anti-node, anti-sovereignty concepts, such as: “federated” sidechains, Fedi, Liquid, etc.
 - Wishful thinking, and other “braindead” advocacy. Stock-to-flow. “Carnivore-style” maximalism, and other cult-like “lifestyle” nonsense.
 - Toxicity, and pointless misanthropy. “We never wanted these users, anyway.” “You’ll come crawling back to Bitcoin, you’ll see!”
 6. Grow the new community.
 - We can only succeed, if we “recruit” people.
 - We need our own “Andreas Antonopoulos”, Roger Ver, Hal Finney, etc. (We also need our own BitPay, Blockstream, Microstrategy, etc.)
 - We also need *new disputes*. For example, a new “Mike Hearn vs Greg Maxwell”. But – this time around – they will settle their dispute *NOT with a new Altcoin*, but with a

new L2, on the same eCash network.

- Prioritize growth. Elevate those who promote *user-adoption*, and shame those who hold adoption back.

A lot of it will happen automatically. Bitcoin has many *serious errors*, which its community is *failing* to address. When the new coin launches, millions of stakeholders will be invited to form an opinion. Among the opinionated, coins will be bought and sold – and the new owners will argue their case (on Twitter and elsewhere). A bright light will shine upon these errors.

It is *these errors* which create our investment opportunity. (Not the brilliance of Bip300.) If Bitcoin were perfect, then no “plan for surpassing BTC” could possibly succeed. But if instead, BTC is *permanently disadvantaged* due to *unfixable cultural errors*, and if there is *a way of getting everyone to notice this*, then there will (eventually) be a stampede to abandon BTC for the nearest viable alternative.

9. If eCash succeeds, won't BTC copy it? Then what?

Indeed – this is a big risk!

We could be *right about everything* – and eCash might still go to zero.

Because: the more success we have, the more attention we will get. If we are *too persuasive*, too early on, then the BTC community may activate Bip300 after all. BTC will then crush eCash with its superior network effects. And we will lose.

So, it's a Catch-22: “lose if you fail; lose if you succeed”.

Actually, it is even worse than that! Since winning is impossible... why would anyone invest? They would not. So, our project will have no effect on the world (even if we were right about everything).

This is a tricky problem to solve...

...but there are solutions:

1. BTC is more rotten than people realize – and much of this rot is cultural (which is not easy to change).
 - In particular, there is a whole “ossification” coalition of Bitcoin; and an “anti-drivechain” coalition. Both are moderately influential. Both will have their reputations damaged, if they have to walk back their anti-drivechain comments. So they will fight tooth-and-nail to keep drivechain away from BTC.
 - Bitcoin has (in large part) ossified already. Where is the next soft fork? (Nowhere in

sight.)

2. Different people, learn at different rates.

- So, when a person learns [that eCash > BTC], they will be faced with a choice: [1] jump ship immediately (and be the first into a new, winning trade); or [2] wait patiently and try to convince others. But, on any single day, only a tiny minority of people will be in the [2] category.
- And – they have to contend not only with [1] the difficulty of persuading others, but also [2] the risk that those others will themselves jump ship (instead of persuade).
- Everyone who jumps ship, will then have an incentive to *delay* drivechain's adoption on BTC – or even to spread *misinformation* about drivechain.

3. BTC and eCash share a mining algorithm (Sha256d). Thus, in the short run, a sudden increase in the blockreward of one coin, will starve its rival of hashrate.

- So, in the early days (while the eCash marketcap is small), "most people" will be skeptical that eCash is better. The risk [of BTC copying eCash] will be low.
- But afterwards, (as the eCash marketcap rises), mining the BTC blockchain might no longer be possible. So, it may be too late [for BTC to copy eCash].
- Even if the eCash marketcap is flat – if eCash *total transaction fees* rise exponentially, then this would also starve BTC of hashrate.

So, the strategies are:

1. Brain drain the smart, creative people out of BTC. Abandon BTC to the crazies, and let them destroy it.
2. Pursue a goal of maximizing the long run total transaction fees paid, per block.
3. "Flip" BTC, via two phases:
 - ■ "Coiling the spring" – a low marketcap phase, where we prepare and strategize with early adopters.
 - ■ "Unleashing the spring" – a phase in which the marketcap surges upward, to attempt to take the #1 spot.

It will not be easy. But it is *possible*. So, investors should be willing to join us – at some price. This resolves the Catch-22.

For more see [Outcomes](#).

10. Can you elaborate on "coiling the spring"?

When network effects are strong, how can you dethrone a larger rival?

In two phases:

1. "Coiling the spring" – In this phase, we purposefully de-emphasize marketing, hype, and

politics – to the point of self-sabotage. We gather evidence, and “stress test” our ideas by trying to falsify them. We are pure [truth-seeking](#); zero teamwork and growth. Pure [scout](#); zero soldier. Pure [mistake-theorizing](#); zero conflict-mentality. We avoid politics – and, in fact, we allow the [sociopaths](#) and parasites to have breathing room, to hopefully trick them into coming “out in the open” – so that we may identify them, and study them, before they become suspicious of us.

2. “Unleashing the spring” – In this phase, we restore politics [and hype and marketing] to their rightful places. Since our idea has been improving *objectively* throughout phase 1, it is (hopefully) now much better. Thus it creates an opportunity, for *new* influencers, promoters, and politician-types to “team up” with the newer, better idea. They have two advantages: [1] they can emulate their BTC-predecessors; and [2] they have a better fundamental idea to work with.

Ideally, by Phase 2, we have paved the way for FAST “viral” growth.

That is the *only* way a new coin can defeat Bitcoin. Early on, it must attract supporters who *expect* future fast growth; later, the fast growth must be *fast enough* to topple the #1 project before it can react.

11. Bitcoin is #1. Always has been – always will be. You can't win!

Bitcoin has been #1 – mostly because of *low-quality competitors*.

Most Altcoins are *pure junk*.

Many have huge premines. Some have *100% premines*: Ripple, Stellar, NXT, Tron, and SHIB. Others, used their genesis block to “distribute to ICO investors” – which is [basically] equivalent to a “100% premine, that is all sold instantly”. These include: ADA, EOS, Aptos, and AVAX. Solana had a 50% pre-mine.

High pre-mines are bad, because they *limit growth* – this kills the project. It caps growth in three ways: [1] it leaves too many people out of the initial coalition, [2] it gives too many coins (as a % of total coins) to the people *in* the coalition (which is off-putting to those of us who must join later), and [3] it invites users to make their own new high-premine coins (favoring themselves, this time). All of this, motivates newcomers to join a coin (or create one), instead of join with the existing coin.

A premine is also terrible, because none of the Altcoins are ever quite finished (nor is Bitcoin). This introduces chaos to the project, as the original founders quit, retire, or are forced out – or various “committees” and foundations appear, to “guide development”. The project drags

on, due to the realities of software development – until morale collapses and the project is abandoned.

In contrast, Bitcoin took a more reasonable path: 0% premine at genesis, 87.5% of the coins released continuously over 12 years. This punishes latecomers appropriately, but not so much that they leave the coalition. The Bitcoin UTXO set (unlike its Altcoin counterparts) has “moral glue” holding it together – those who bought Bitcoin, partly embrace a *shared vision*. (In Bitcoin’s case: a world without the banks.) It is a team effort.

A “hard fork” preserves this UTXO set. This automatically puts it in a different category.

BCH we have already discussed (in question 7).

BSV is a fork of BCH (not BTC), and its litigious and ridiculous founder has speedily driven away all reasonable people. The other forks (“BitcoinGold”, “BitcoinDiamond”, etc), are frivolities. They were not legitimate competitors to BTC. They did not aspire to be the #1 coin. They were created because people wanted free money; and because it was easy to recompile the software with a new name. In fact, many of them were (I assume) created to de-legitimize BCH (with the goal of muddying the waters, in that debate). Therefore, out of all the hard forks, only BCH presented a serious *vision*. The others are knockoff cash-grabs. (We discussed BCH in question 7.)

We now turn to Ethereum – the #2 coin. It has differentiated itself [from Bitcoin], in many ways: proof of stake; frequent hard forks (ie “mandatory upgrades”); account model (vs UTXO); aggressive culture (vs conservative); fast block times; uncle blocks rewarded; higher node costs (and less discipline in capping node costs); Turing-complete EVM scripting. All of those changes... are bad. Ethereum exists because developers love to create stuff and have fun (which is understandable) – but drivechain is better for that. Drivechain has no gas fees. Each L2 has its own chain, and does not share a chain (nor a fee-rate) with any other chain/contract.

So, in general: there has been a depressing lack of seriousness among the Altcoins. A handful – Ethereum, Monero, Namecoin, zCash – have an actual *vision* for the world. The rest are just get-rich-quick schemes, or hobbyist projects.

The low quality of today’s Altcoins has –lamentably– contributed to Bitcoin’s complacency. With no competitors to keep it honest, Bitcoin has mostly wasted the last 10 years.

12. What would convince you NOT to go through with this hard fork?

Well – one thing, could be for 51% BTC hashrate, to activate Bip300 (on BTC). That might

render eCash useless.

Bip300 is an opt-in, reversible, soft fork. With the CUSF client, miners can start/stop it at any time. Plus, Bip300 (hopefully) gets them more money – much more money.

The bigger problem is the community. Without a community of *genuinely interested* users, the mere activation of Bip300 will do very little.

13. What do you think of BitVM / zk-Rollups / new technology? How do you feel about your competition?

This is already answered in [FAQ - #comparables](#).

But – more importantly – Bitcoin does NOT have any **tech problems**. It does NOT have any technical limitations. The *existing software stack* is already sufficient to achieve unlimited scale, privacy, programmability, interoperability, extensibility, ossification, etc.

But, what Bitcoin DOES have is **cultural problems** – also known as [the derangements](#). That is why we need a new project. It has nothing to do with technology.

14. The drivechain idea is over 10 years old. If it were good, someone would have used it by now. Hasn't the moment passed?

The Drivechain-inventor was [the first proponent of blockchain prediction markets](#), back in 2012. PolyMarket finally went mainstream in 2024 – over 10 years later.

The drivechain idea [has many supporters](#) – including most of the crème de la crème of the Bitcoin world.

By comparison, the Lightning Network is also 10+ years old.

	Lightning	Drivechain
Age	10+ Years	10+ Years
How many devs?	50+ full time, 100+ hobbyists, 5+ generational-talent level geniuses, 5+ big SF co-founders.	2 people, working casually in their spare time. Eventually, maybe 10-12 more.

	Lightning	Drivechain
How much money invested?	Much more than \$100 million.	Less than \$4 million.
How much attention / praise / media support?	Enormous, fawning support – full blown 10+ year propaganda campaign.	Minimal amount.
Can you build a demo of it, working for 8 billion users.	No – because this is not possible with Lightning.	Yes – and we already have .
Is this idea ultimately going to work?	No. It will not.	Yes, it might.

In Oct 2025, the Drivechain-inventor [debated a room full of LN devs](#), at TabConf (the #1 Bitcoin developer conference). Tadge Dryja (the inventor of LN), joined him on stage in the final 10 minutes – and ultimately accepted all of Paul’s critiques.

Yet, people continue “trying” the Lightning Network. This is not because LN is a good idea. It is because they are too embarrassed to admit their past mistake(s). They pass over good ideas (such as Drivechain) for the same reason.

In fact, most critics of Drivechain, admit that they have never actually read [the BIP text](#) (which is only a few pages long). So: Bitcoin is not a meritocracy. It is a bureaucracy. The problems with Bitcoin are not technical – they are cultural.