The Bitcoin Blackpaper

Maitreya Lockwood
www.kymafi.com

Abstract. A truly decentralized protocol and monetary system does not require a financial institution or a third party entity. Bitcoin, as described in the whitepaper by Satoshi Nakamoto, was originally designed to be a Peer to Peer Electronic Cash System. We propose a solution to the corruption of the Core Bitcoin client and its attack on the honest nodes by activating a hardfork on September 1st, 2026. We maintain that this will be the longest chain and retain the name of the Decentralized Money as long as it adheres to its original telos, remains decentralized and secure. We claim this name to be our right to hold as honest node runners. Any chain that claims this legacy while not adhering to its consensus rules will not be recognized as valid by our network.

1. Introduction

Bitcoin is not a ticker symbol on a corporate exchange. It does not have a website or domain name. It is not an asset, a stock of speculation nor is it a database for non-monetary data. Bitcoin is a set of consensus rules, a sovereign network, and a technological promise. When we initiate this hard fork, we are not creating a new asset; we are correcting the course of the existing one. Therefore, we will not change the name, nor will we concede in the future. The name "Bitcoin" is rightfully ours by virtue of adherence to the original principles of the protocol.

We are witnessing the capture of the opposing chain by non-monetary actors, institutional bloat, fiat corruption, inflated supply from paper contracts and custodial convenience lacking proof of reserves. The legacy chain has become a vehicle for IOUs and KYC-controlled speculation. We refer to this bloated and inflated chain as Illegitimate. This is a recognition that when a network prioritizes high time preference, data-heavy traffic over peer-to-peer monetary utility, it has fundamentally ceased to function as sound money. Therefore that chain cannot honestly be recognized as coinage, a monetary system, or a medium of exchange, while it makes alternative use cases and inflates supply. It most certainly cannot claim to be Decentralized Peer to Peer Electronic Cash.

2. Transactions

We acknowledge the reality: centralized exchanges will attempt to dictate the naming convention. They will likely list our chain under an alternative ticker to maintain their hold on liquidity. We do not consent to have our monetary protocol listed. We do not lobby for listings. Instead, we adopt a posture of absolute non-engagement. Our brand and ethos are the rejection of the exchange-captured IOU model, the ETFs, the Treasury and Bitcoin-to-Fiat Lending Companies.

We henceforth do not recognize any coin that is exchanged outside the network in the form of paper contracts, IOUs, or non self custody. Any institution that lists these tokens is in direct violation of the protocol, and is an attack on the network.

3. Strategy

We did not intend for the Bitcoin network to suffer a chain split. Our network of nodes reached overwhelming consensus led by a movement to preserve its monetary principles. This was originally proposed in a Reduced Data Temporary Softfork also known as BIP110. No URSF was ever activated. Instead the network was attacked from all angles. We were censored online, removed from the forums, and our developers were even removed from the BIP editorial team.

During the softfork, we came across a harsh reality. The mining pools which run on the SHA 256 algorithm have largely centralized. During the time leading up to the activation date, two pools often controlled over 50% of the hashrate. A total of just 6 pools controlled over 70%. Despite any URSF, these mining pools colluded and began attacking the network on August 8th, 2026, causing a chain split.

And so, as honest node runners and defenders of this Protocol, we now extend our right to hardfork their chain. These mining pools will no longer be mining valid blocks on the Bitcoin Network. We do this by activating a new Proof-of-Work algorithm which was fairly and randomly selected. Luke Dashjr and the organizers created a mapping file that assigned each possible concluding hexadecimal character of a block hash to a specific candidate algorithm. They published a SHA-256 hash of this file beforehand to prove it was locked and could not be altered. The rule dictated that the final algorithm would be chosen based on the last character of the block hash of the very first Bitcoin Testnet4 block mined after a strict 14:00 UTC deadline. When the designated Testnet4 block was mined, its hash ended on the specific character that mapped to BLAKE2b.

By altering the Proof-of-Work algorithm, we lower the barrier to entry. Every node operator becomes a miner. We do not rely on centralized data centers. We bypass fiat on-ramps by building a native circular economy. If you want Bitcoin, you mine it, you work for it, or you trade for it directly. You cannot buy it for fiat from a custodian who holds your keys.

4. Conclusion

We have proposed a system for electronic transactions without relying on trust, and now aim to retain that sovereign right to the name and protocol. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but it is incomplete without preserving it as strictly a monetary protocol. It was captured by third party institutions, a corrupted and misaligned client and centralized miners. We dismiss the arbitrary data that degrades the network, and bears a heavy burden on node runners. We fully reject collusion of mining pools and the centralization of block mining on the SHA256 algorithm. To solve this, we proposed a new proof-of-work algorithm to record a public history

of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. We will retain the name, the transaction history and preserve its original telos. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

And this is the consensus reached by the nodes of the network:

THIS PROTOCOL WILL BE CALLED BITCOIN.
PEER TO PEER DIGITAL CASH.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, 2008.