Defense by Hash War

JAVIER GONZALEZ GONZALEZ
the@nakamoto.observer

1. Introduction

Satoshi Nakamoto designed Bitcoin specifically **to not be controlled** by a central authority. Not even himself. That's why he invented "the miners" as the executive power of Bitcoin, and then disappeared.

External actors —whose unverifiable power emanates from nowhere— will attempt to take control of the Bitcoin blockchain. This has been tried in the past and will be tried in the future cyclically.

But with hashpower Miners can coordinate the necessary defense of the Bitcoin blockchain, which is the miners' business. With a skillful execution. Taking political-economic risks. In a counter-intuitive, sophisticated, peaceful and disruptive cybersec operation called Hash war.

2. Quotes

Any needed rules and incentives can be enforced with this consensus mechanism.
Satoshi Nakamoto (the first Bitcoin miner) 2009-10-31

Miners are the only party that could vote and therefore miners would decide.
Chun Wang (F2Pool) 2015-12-07

Preventing a minority-hashrate fork from confirming any transactions is a good idea.
Gavin Andresen (Lead developer) 2017-02-04

It may not be necessary to attack it. But to attack it is always an option.
Jihan Wu (Bitmain, Bitdeer) 2017-03-21

The answer is simple: because the hash rate can kill a chain.
Jiang Zhuoer (BTC.TOP) 2018-11-14

BCH / BSV Fork (Hash War) - - $ 952,926.48
Roger Ver (Bitcoin.com) 2020-01-17

Large blockers had allocated a budget of US$100M to attack the smaller blockchain.
Jonathan Bier (The Blocksize War) 2021-03-14

3. Glossary

- **Bitcoin**
  A decentralized consensus mechanism enforced by hashpower.
  Started by Satoshi Nakamoto -the first miner- to accomplish the global adoption of:
  “Bitcoin: A Peer-to-Peer Electronic Cash System”
  `b1674191a88ec5cdd733e4240a81803105dc412d6c6708d53ab94fc248f4f553` Whitepaper
  `000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f` Genesis Block

- **Decentralization**
  Building something you don't control.

- **Miners**
  Who ultimately controls a percentage of hashpower.

- **Hashpower**
  Computational power universally-verifiable with a hash algorithm as a Proof-of-Work.

- **Executive Hashpower**
  When miners decide to act with hashpower, ignoring markets temporarily, not following short-term benefit, but a potential future major profit. Mining at loss. Causing a disruption in DARI.

- **DARI** (Difficulty Adjusted Reward Index)
  A ratio to compare the rewards of two blockchains that share the same hash algorithm.
  $DARI = (Coinbase + Fees) \div Difficulty \times Fiat\ exchange\ rate$

- **Hash war**
  When two opposing forces of Executive Hashpower collide for a political power dispute. This is how rules and incentives can be enforced with this consensus mechanism.

- **Reorg** (blockchain block reorganization)
  When the last blocks of the chain are replaced by others by a major hashpower force, rewriting and changing the destiny of the blockchain.

- **Empty blocks**
  Blocks without transactions (except coinbase transaction). If all new blocks are empty then the blockchain stops working. No user loses money. No double-spends.

- **Main chain**
  The blockchain defended by the majority of hashpower.

- **Minority split**
  The blockchain defended by the minority of hashpower.

- **The Nakamoto Consensus**
  The majority of hashpower as a new form of executive power. A decentralized authority. The consensus mechanism is through hashpower voting by simple majority (51%).

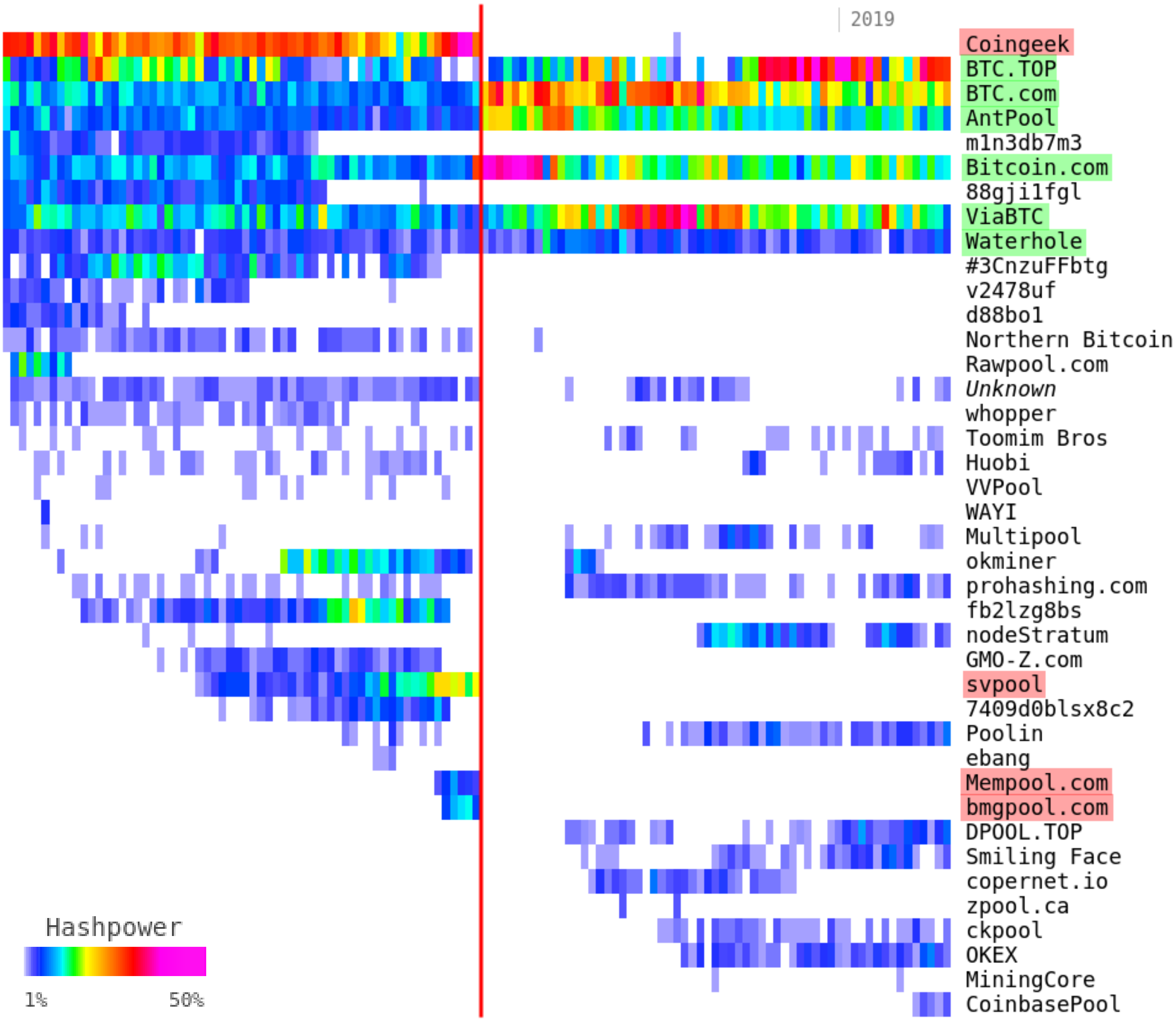
4. Precedents

1) On November 15, 2018, the first Bitcoin hash war occurred, in Bitcoin Cash block 556767.

The power dispute was declared by a belligerent force that days before the event had a majority of hashpower in BCH. But during this hash war the 14% of BTC hashpower moved to BCH, mining at loss, ignoring the market price in short-term.

The result was the victory of the BCH miners.
Leaving BSV as a minority split.

Belligerents	
Bitcoin.com	nChain
Antpool	Coingeek
ViaBTC	Others
BTC.com	
BTC.TOP	
Others	



2) On November 28, 2020, a hash war occurred in eCash (XEC) block 662397.

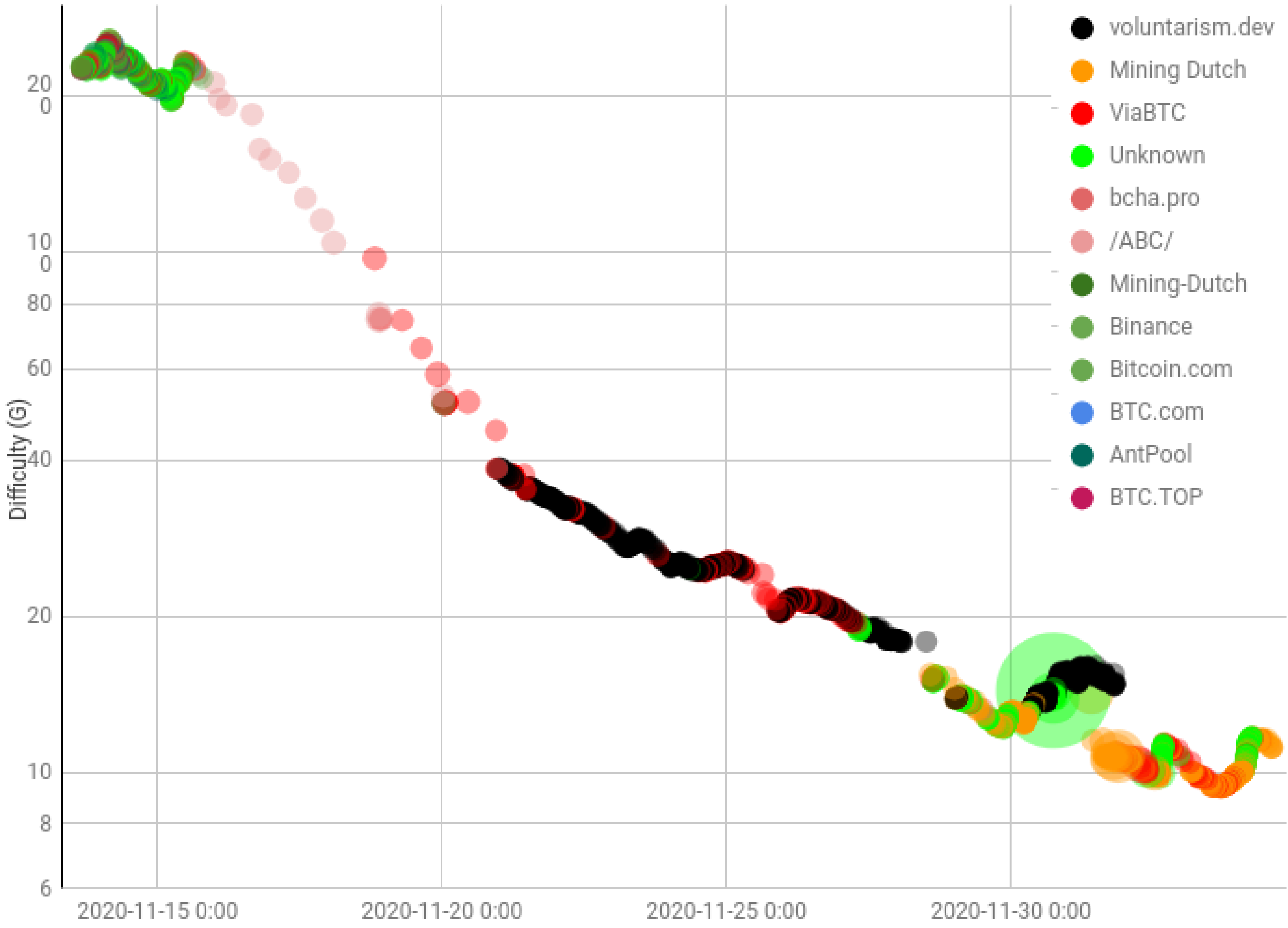
The power dispute was declared by Bitcoin ABC central devs attempting to unilaterally capture 8% of the coinbase incentive, which belongs to the miners, causing a third split in BCH.

Belligerents	
voluntarism.dev	Bitcoin ABC ViaBTC Mining-Dutch

As retaliation, an anonymous small mining force started a hash war on XEC (then known as BCHA) making empty blocks and reorg sustained for 28 hours.

After a centralized “invalidateblock” the hash war was stopped and was not continued. Possibly due to lack of consensus to continue the action to the end.

The result was the capture of the 8% of miners incentive by Bitcoin ABC causing a split.



Each circle is a block, the size is the number of transactions.
More details in: https://nakamoto.observer/executive_hashpower

5. Victory Conditions

1. Original market ticker preserved by the main chain.
2. The majority of hashpower criteria prevails in the main chain.
3. Main chain operating normally without disruption.
4. Stopping a minority split, with empty blocks and reorg, until this points are met.

6. Legitimacy and Limits

For a miner's incentive to exist, it is not enough to publish the next valid block before anyone else. It is also necessary that the majority of hashpower decide voluntarily to work on continuing exactly that block. It is a voluntary consensus, non-violent, without coercion.

Executive Hashpower actions	**Possible**	**Legitimate**
Coordination by Coinbase Signals	Yes	Yes
Empty Blocks	Yes	Yes
Reorg	Yes	Yes
Empty Blocks + Reorg (no split)	Yes	Yes (1)
Bandwidth DDoS	Yes	**No** (2)
Double-spend	Yes	**No**
Reorg in a different Genesis Block	Yes	**No**
Reorg in a different PoW algorithm	No (3)	Yes

(1) It is legitimate inside the opportunity window between the first minority split block and the opening of markets (days or weeks later). Making consecutive empty blocks until the main chain prevails, completely stopping the operation of the minority split. In this case, for users, it is like nothing has happened. In other cases can be controversial.

(2) Hash war is not a ”distributed denial-of-service attack”. During a hash war there is no CPU or bandwidth usage collapse. The Internet suffers no harm. Hash war is a legitimate consensus mechanism exactly as Bitcoin was designed.

(3) In some cases, with sufficient funds, it is possible with rented hashpower.

7. The Narrative

Miners must satisfy holders in the long-term, but in the short-term only hashpower can resolve disputes acting as executive power. Hash war is about actions prevailing over words. Putting an end to social engineering. However, no one should do hash war without a clean and meaningful communication strategy.

Each belligerent party will try to propagate its own narrative, where they are the good people who must win and the other party are the bad attackers who must lose. The narrative is part of the field of social engineering, where also deception and lies operate. In addition, cultural and language differences add interferences.

Hash war without a good narrative is like sailing against the wind. It is possible, but it is not efficient. Miners should publish a unified, simple and direct messages about what is going to happen and why.

Examples

✖ To attack by hash war it is always an option.
✔ A defense by hash war it is always an option.

✖ We want blocks of 2 MB, 4 MB or 8 MB, or dynamic size.
✔ We want 2 MB blocks for now.

✖ To kill a chain.
✔ To stop a minority split with a decentralized consensus mechanism.

✖ We will make empty blocks ad-infinitum.
✔ We will make empty blocks only when the minority force makes a new block.

8. Economics

Making hash war may seem expensive, but miners can take a loss in short-term to avoid a much larger loss in long-term.

For example, the profits for a globally adopted Bitcoin useful as gold and cash at the same time is immense and protecting this goal will be worth it at any cost.

Miners need to be well coordinated to act together and bear the costs in proportion to their hashpower. If a miner controls 1% of the hashpower, he must bear 1% of the costs of mining at a loss to make the hash war.

9. Hypothetical Scenario

> This is a hypothetical worst-case situation where a hash war defense is necessary and recommended. This is fictitious and any similarity to reality is coincidental.

Intel agencies have early detected the exponentially growing of adoption as currency of an open-source project called Bitcoin. For these organizations, the remote possibility of losing the prerogative to print money in the future is totally unacceptable and a matter of survival for their hegemony. Therefore, they intend to stop the Bitcoin project in the most efficient and least costly way, as soon as possible.

First, they intercept the founder of the project to extract information and try to impersonate him. Then they use this info to damage the reputation of the second lead developer to kick him out of the project. But this does not stop the project. It is decentralized and, like the Internet, it is designed to survive a network decapitation.

The next strategy consists in creating a private company to involve some central devs who control the project's code to constitute a cartel to prevent the expansion of the block size at all costs. Including complementary attacks such as social engineering, damaging the reliability of 0-conf transactions and making DDoS attacks against the opposition. This limits the capacity of the network to only five transactions per second. Raising fees exponentially and destroying Bitcoin's adoption as cash.

The majority of hashpower identifies this as a threat by an external actor. Miners consider that this significantly alters the course of the project and if attempted it should be done in a new project with a different Genesis block. This threat means the capture of future fees that legitimately belong to the Bitcoin miners. It foresees a fracture in the community and irreversible damage to the project, including the destruction of adoption, which means the utility and is the main foundation of the long-term value.

Therefore, to revert the central devs takeover and regain the control of their own project, the Bitcoin miners decide that it is time to make a defense by Hash war.

10. Hash War Training

If you want no split, prepare for hash war.
Miners must be ready for hash war at any time.

The hash war must be automated to make consecutive empty blocks with reorg relentlessly, quickly and only when necessary.

The central devs of the minority split will desperately try to deflect the effects of the hash war in an authoritarian manner through “invalidateblock” and similar illegitimate tactics. Therefore, miners will be prepared to act quickly, within minutes, adapting the action to persist in the face of any evasive maneuver. Ensuring the creation of the minimum necessary amount of empty blocks and in the right split, causing the total dysfunction of the minority split.

At the end of the day, since code obeys hashpower, central devs will not be able to prevail.

It is absolutely necessary to train a team of specialized operators in previously performed hash war games. And also to develop specific and flexible software elements for hashpower executive actions in a battle context.

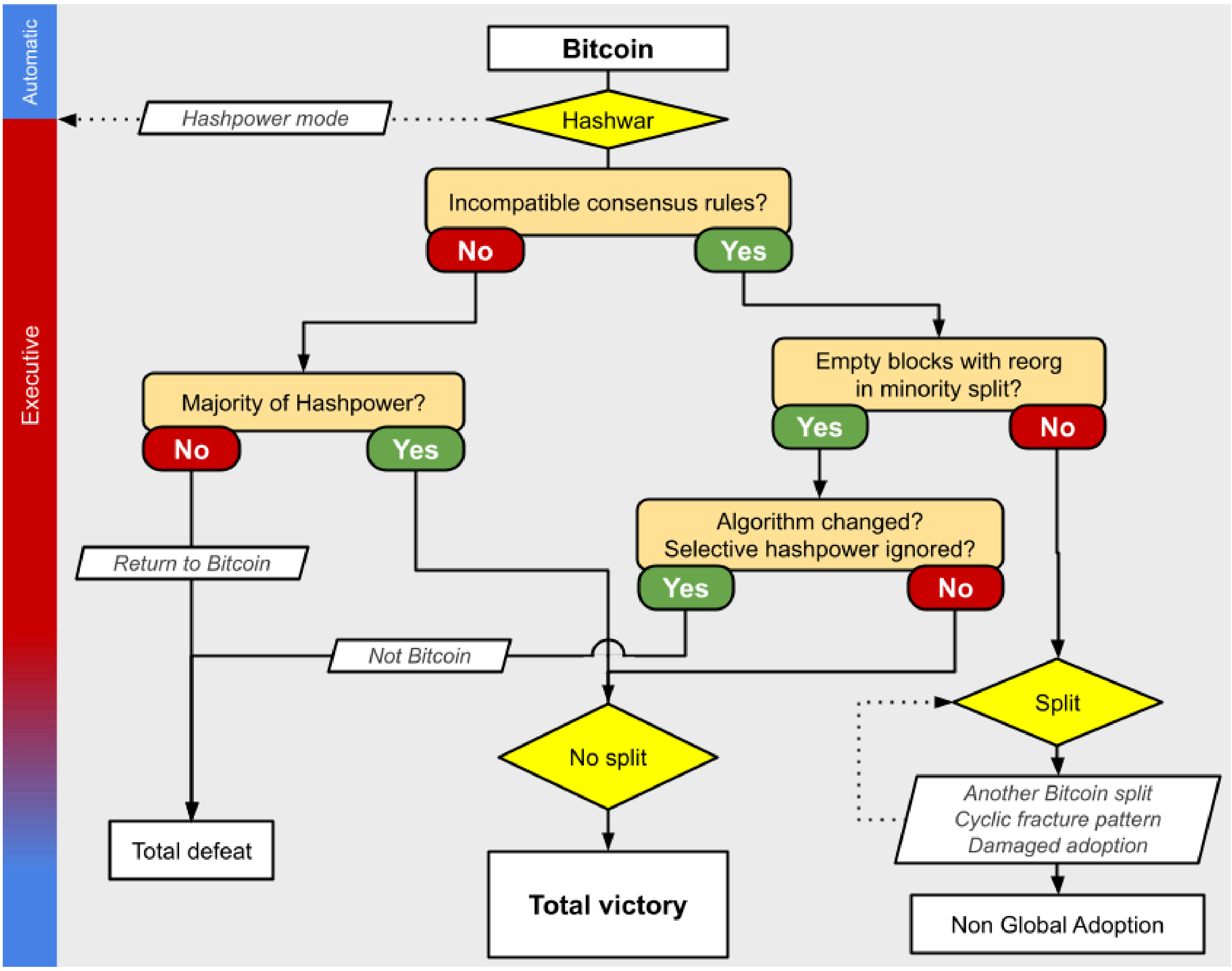
Hash war games should be played simulating a defensive blue team trying to protect and upgrade the main chain without split. And a red team trying to prevent the upgrade trying to make their minority split prevail. The blue team will always have a majority of hashpower.

11. Hash War Checklist

- □ When off-chain diplomacy fails.
- □ Never act in minority of hashpower.
- □ A coalition of allied miners greater than 66% of hashpower.
- □ Hashpower votings to discover consensus.
- □ Agreed determination to accept short-term losses for long-term benefit.
- □ Team of hash war-trained pool operators ready.
- □ Public relations team ready.
- □ Key personnel well coordinated with relays to act 24/7.
- □ Redundant critical infrastructure.
- □ Additional server infrastructure ready.
- □ DDoS protections activated.
- □ Anonymous mining mode ready.
- □ Executive Hashpower ready.

12. Hash War Execution

1. To talk and vote with hashpower to discover the Nakamoto Consensus.
    a. It must be on-chain, off-chain meetings are only complementary.
    b. The most sophisticated way is to use the BMP protocol.
2. Anticipated intentions announced on-chain.
    a. Exhibiting a coordinated majority of hashpower.
    b. Publicly explaining what is going to happen and why.
    c. Providing arguments when necessary.
    d. Public communications always on-chain.
3. Fork and publish the new Bitcoin software version.
    a. Signaling on-chain the hash of the new software.
4. Start anonymous mining.
5. Protect the main chain.
    a. Keeping stable the flow of blocks with transactions.
    b. Reverting possible reorgs.
    c. Reverting possible double-spends.
6. Neutralize the minority chain.
    a. Stopping the transactions in the minority split.
    b. Making empty blocks with reorg in a row.
    c. Stopping the creation of empty blocks periodically to see if the split persists.
    d. Monitoring any adversary actions.



13. Hash War Resolution

The hash war will end when the minority chain stops creating new blocks with transactions, assuming defeat and ceasing to exist.

Then, exchanges and other providers will then have no choice but to accept the new software update respecting the majority of hashpower, also know as The Nakamoto Consensus. Following the fundamental principle that Bitcoin software obeys hashpower. As designed by Satoshi Nakamoto, the first Bitcoin miner.

Victory can be declared when major exchanges resume operations accepting the main chain transactions with the miners software update. Being the time to celebrate the decentralized and peaceful dispute resolution.

14. Conclusion

The Bitcoin miners play a pivotal role. As custodians of the network's security and integrity, they are not just passive entities focused on profit. Instead, they are an essential part of the dynamic that maintains the ethos of decentralization.

Their ability to engage in Hash war is not an act of aggression but a tool for defense, ensuring the protocol remains pure and free from external interference.

While Hash war may be seen as a combative tool, it is fundamentally a defensive strategy. It defends the very principles upon which Bitcoin was founded, and by extension, the broader ideals of a decentralized future where power is distributed and not centralized.

Like a digital version of natural selection, Hash war represents a non-violent contest of ideas and resources, ensuring that only the fittest version of the blockchain will succeed. It's a reminder that in the end, Bitcoin's course is not determined by whimsical market sentiments or individual agendas, but by a majority consensus, achieved through raw computational power and strategic alignment.

This consensus mechanism serves as a bulwark against centralized control, maintaining Bitcoin's promise as a truly decentralized peer-to-peer electronic cash system.

2023
the@nakamoto.observer
gonzo@virtualpol.com
A3AD 4AC5 F252 8190 65A5 75A0 B9C3 5FBF 43B3 19C2

References

- https://nakamoto.observer/bitcoin.pdf
- https://medium.com/@jiangzhuoer/abc-vs-bsv-hash-war-part-iii-the-war-of-the-hash-power-45fef8010467
- https://read.cash/@Jiang_Zhuoer_BTC.TOP_CEO/bch-miner-donation-plan-update-0cf20809
- https://nakamoto.observer/static/papers/Miners_are_the_executive_power_of_Bitcoin_EN.pdf
- https://nakamoto.observer/static/papers/BMP_EN.pdf
- https://read.cash/@JavierGonzalez/executive-hashpower-97e56ffb
- https://read.cash/@JavierGonzalez/miners-empowerment-rules-55374dd5
- https://read.cash/@JavierGonzalez/why-bitcoin-cash-need-the-bmp-1a6ab975
- https://read.cash/@JavierGonzalez/verifying-an-on-chain-bmp-vote-5f3cad2a
- https://twitter.com/JavierGonzalez/status/1591731317909385216
- https://bmp.virtualpol.com
- https://nakamoto.observer