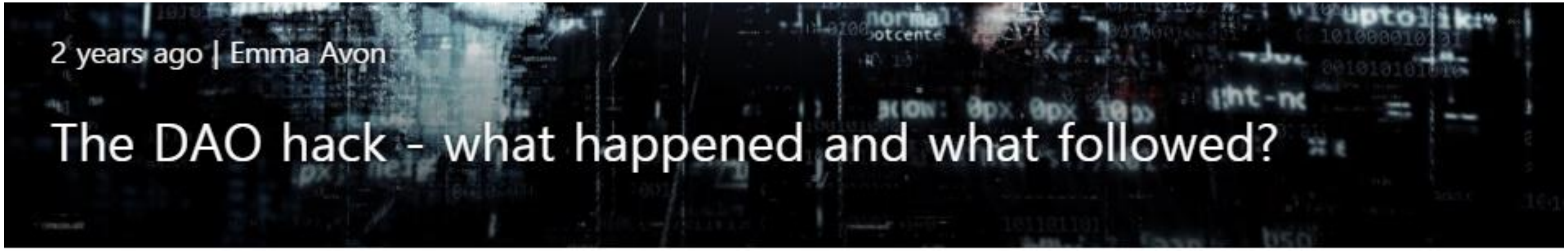
Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash?

Yujin Kwon*, Hyoungshick Kim°, Jinwoo Shin*, Yongdae Kim*

*KAIST, ° Sungkyunkwan University

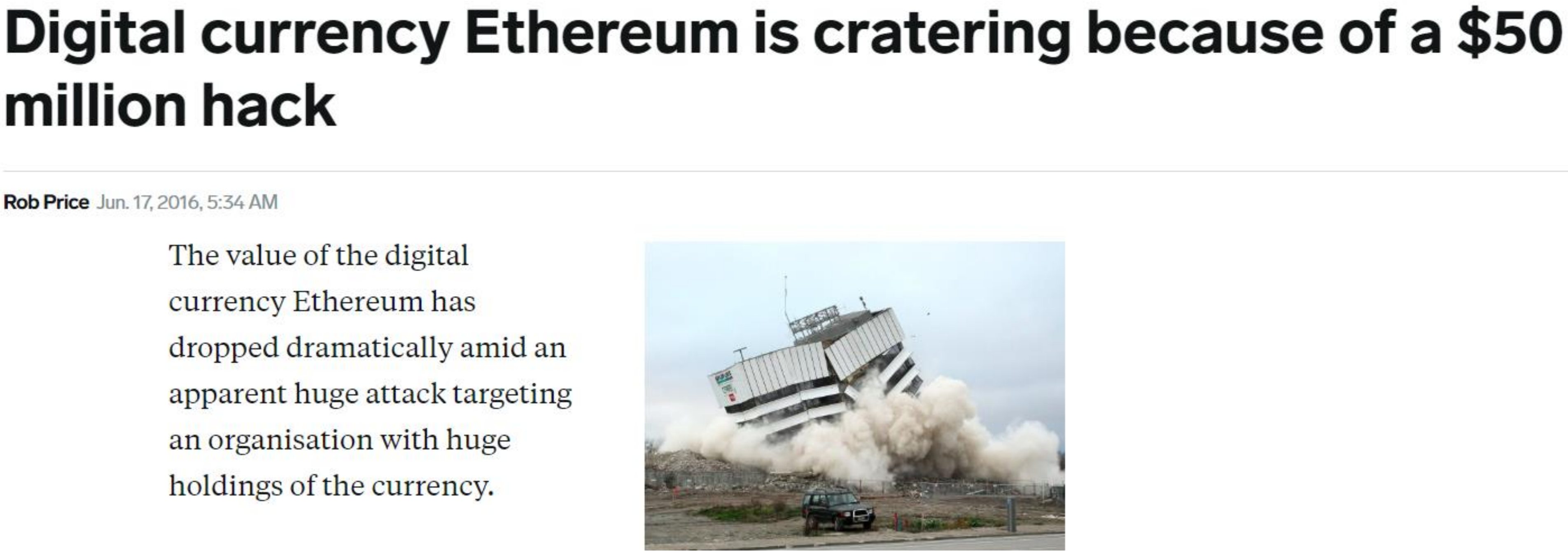
Government conflict



2 years ago | Emma Avon

The DAO hack - what happened and what followed?

In 2016 a grand idea
Organization (The D
cryptocurrency proje
had a creation perio
exchange for DAO t
approximately $150M
the cryptocurrency s



Digital currency Ethereum is cratering because of a $50 million hack

Rob Price Jun. 17, 2016, 5:34 AM

The value of the digital currency Ethereum has dropped dramatically amid an apparent huge attack targeting an organisation with huge holdings of the currency.

Governance conflict

2 years ago | Emma Avon

Th

How did they resolve this crisis?

a $50

In 20
Org
cryp
had
exchange for DAO tc
approximately $150N
the cryptocurrency s|

currency Ethereum has dropped dramatically amid an apparent huge attack targeting an organisation with huge holdings of the currency.

Governance conflict

2 years ago | Emma Avon

Th

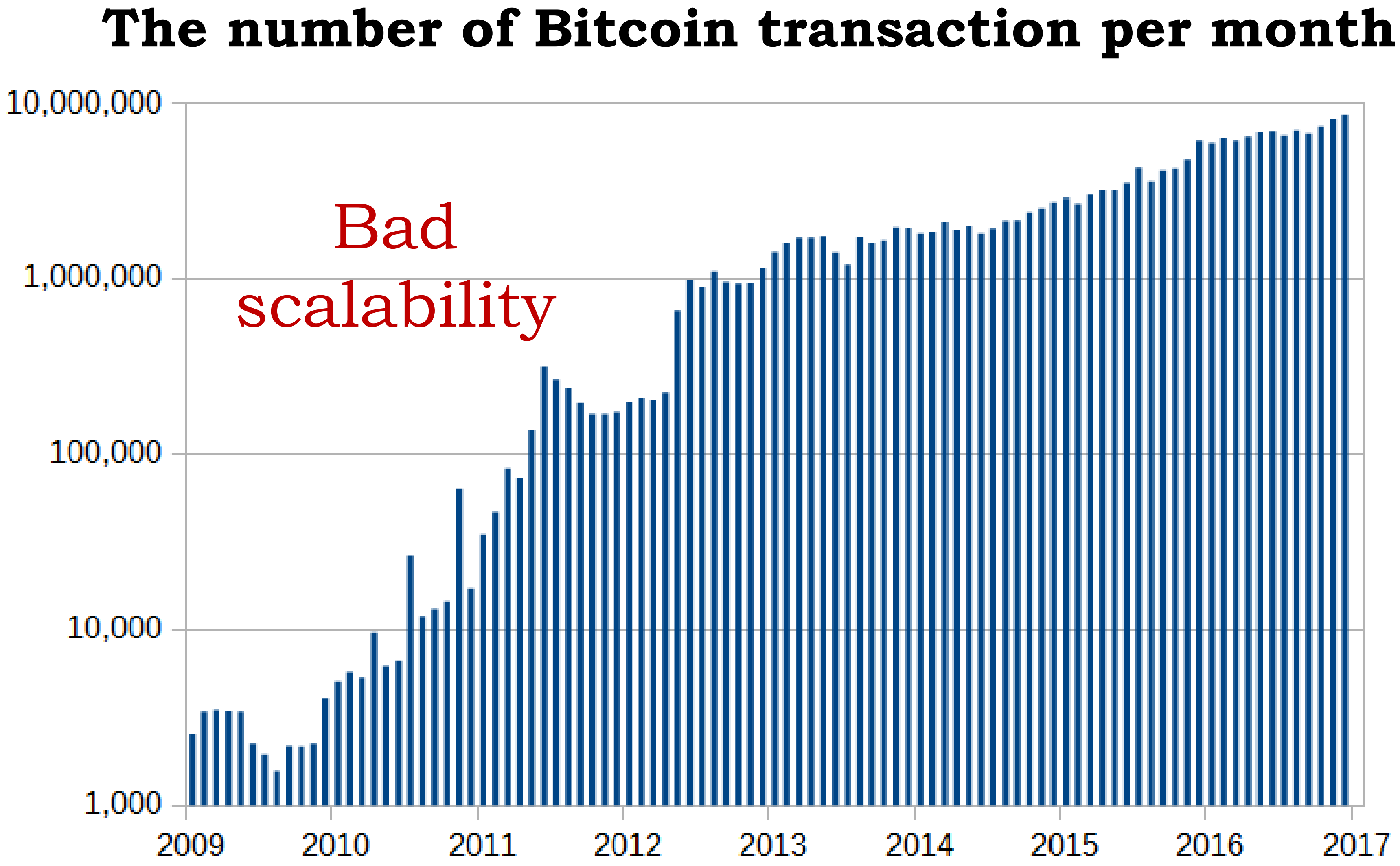
Eventually, Ethereum was split into ETH and ETC.

a $50

In 20
Org
cryp
had
exchange for DAO tc
approximately $150N
the cryptocurrency s|

currency Ethereum has dropped dramatically amid an apparent huge attack targeting an organisation with huge holdings of the currency.

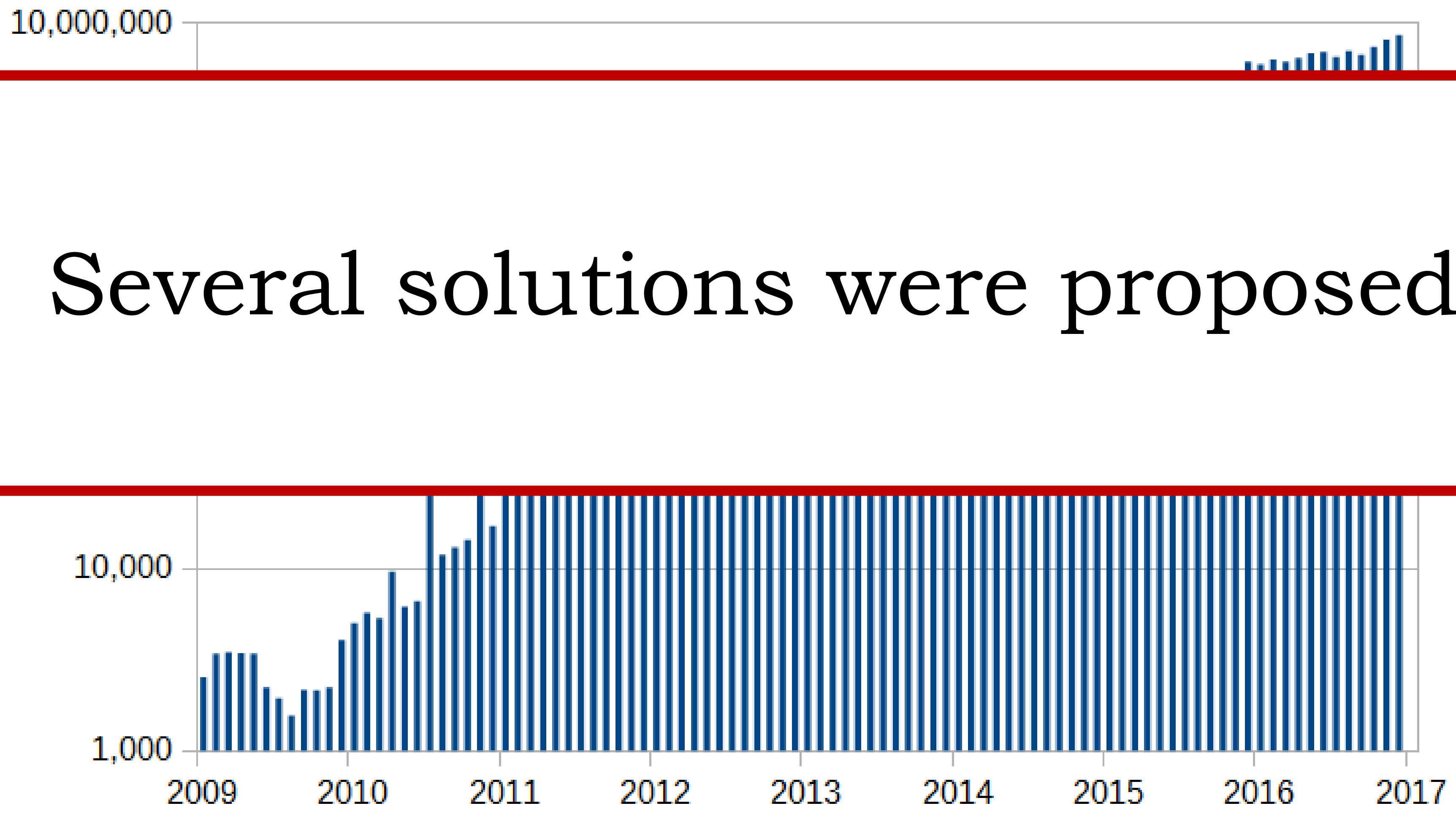
Governance conflict



Bad scalability

Governance conflict

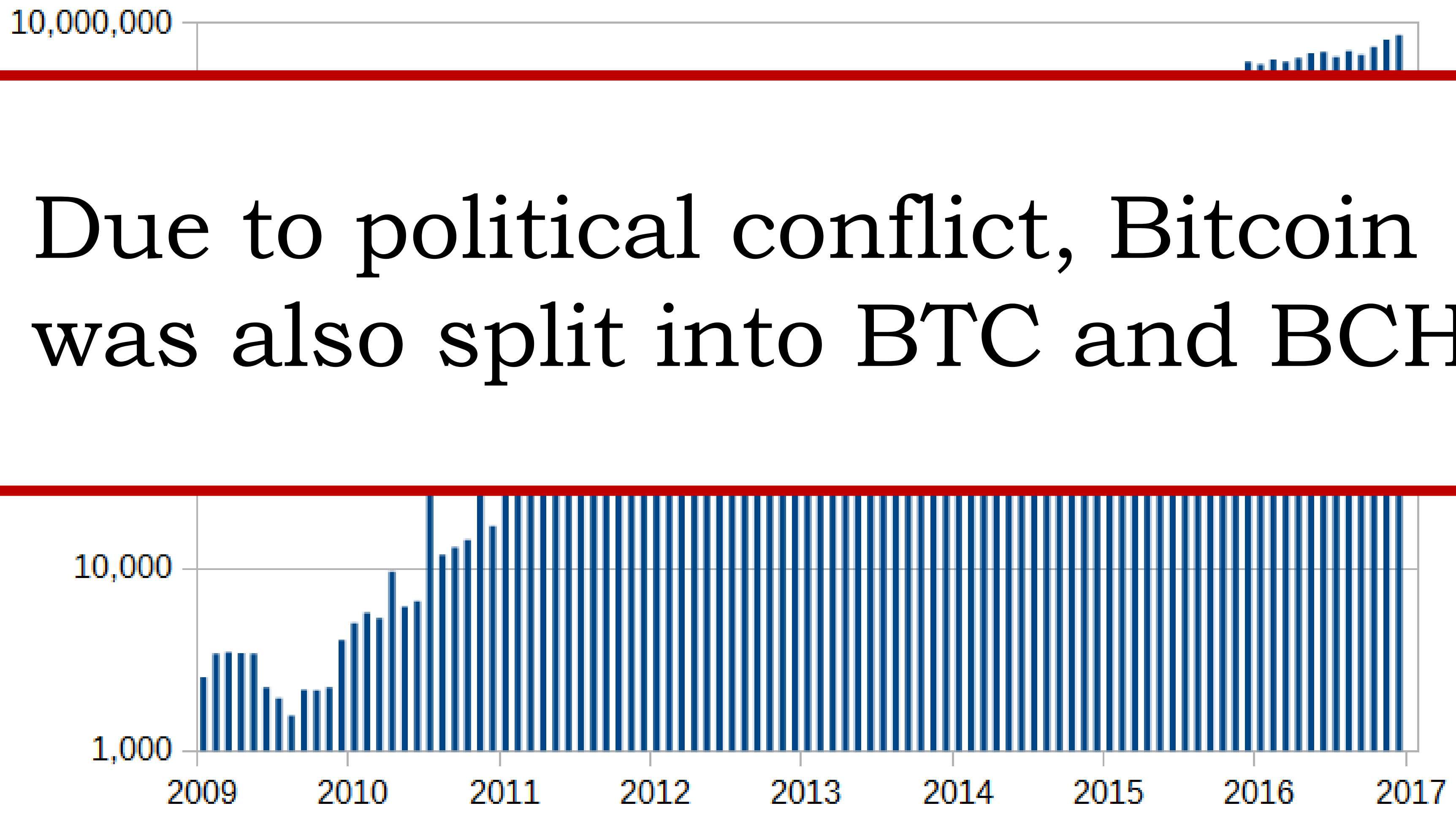
The number of Bitcoin transaction per month



Several solutions were proposed.

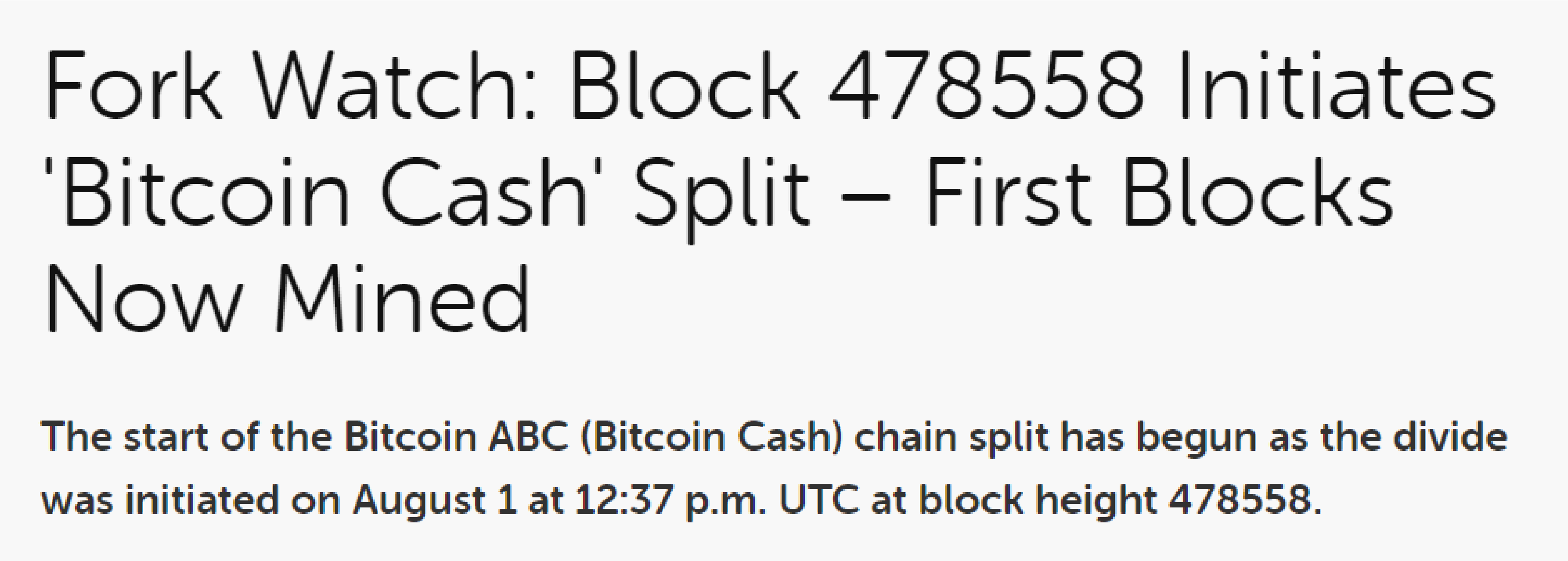
Governance conflict

The number of Bitcoin transaction per month



Due to political conflict, Bitcoin was also split into BTC and BCH.

BTC vs. BCH



Fork Watch: Block 478558 Initiates 'Bitcoin Cash' Split – First Blocks Now Mined

The start of the Bitcoin ABC (Bitcoin Cash) chain split has begun as the divide was initiated on August 1 at 12:37 p.m. UTC at block height 478558.

- Simple idea: Increase a block size
  - BTC: 1 MB/ BCH: 8MB
- They have a **compatible mining algorithm**

How can miners behave?

Fickle mining

- ❖ Depending on profitability of coin mining, miners can dynamically switch the coin to be mined.

When it is more profitable to conduct BTC mining

Bitcoin (BTC)

Bitcoin Cash (BCH)

Fickle mining

- Depending on profitability of coin mining, miners can dynamically switch the coin to be mined.

When it is more profitable to conduct BCH mining

Bitcoin (BTC)

Bitcoin Cash (BCH)

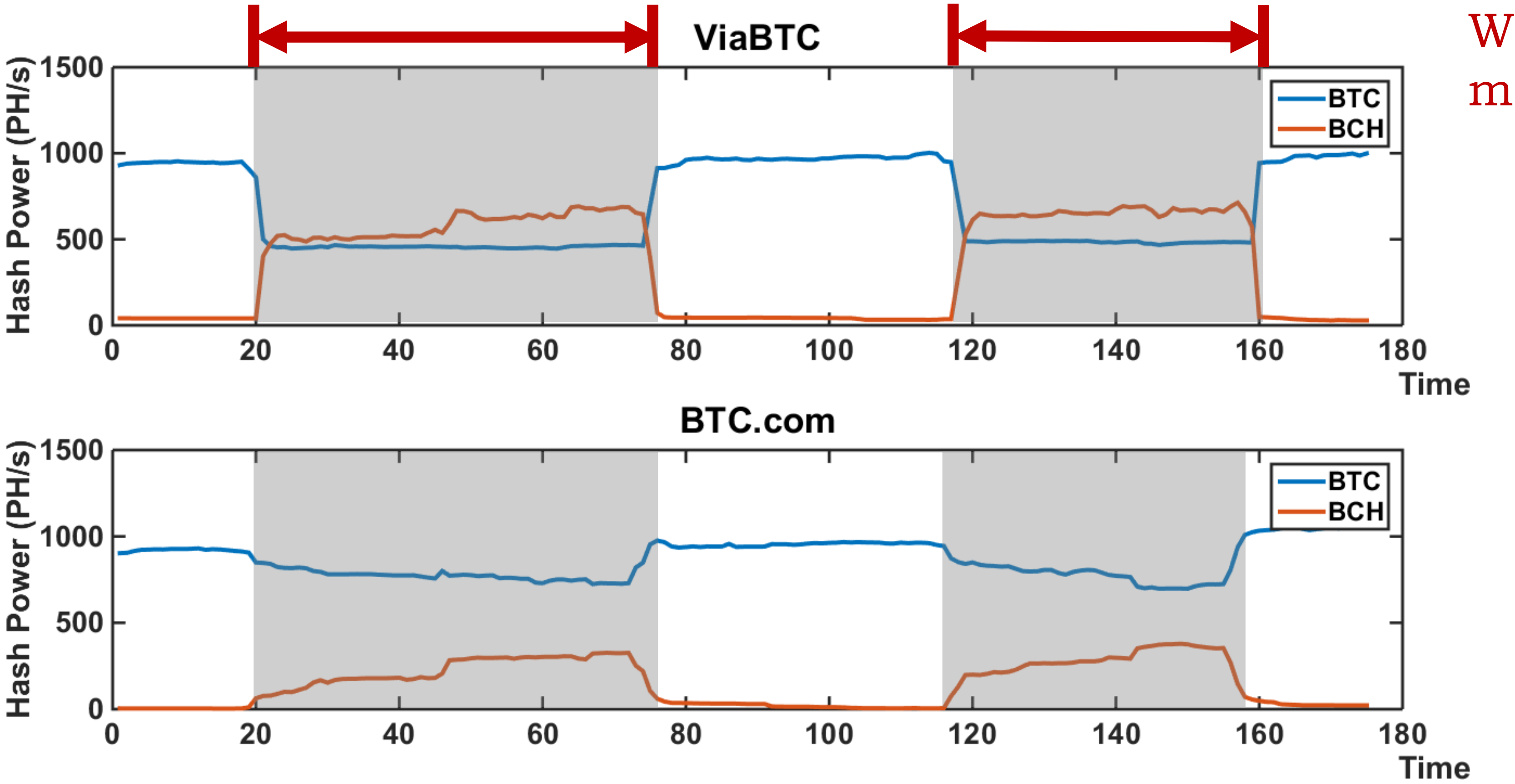
Fickle mining

- Even though the coin mining profitability depends on both the coin price and mining difficulty…

It is hard to predict the coin price.

Oh! I think I can predict when the mining difficulty changes.

Fickle mining

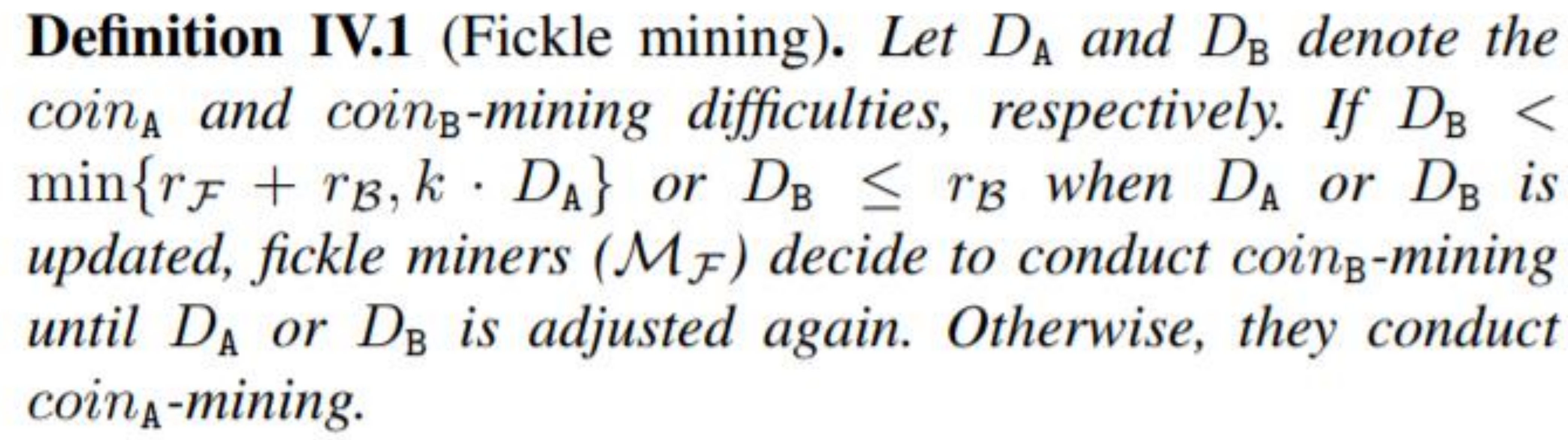


When BCH mining is easy

- ❖ When the BCH mining difficulty becomes easy, large hash power moves from BTC to BCH.

Fickle mining

- ❖ The following strategy is referred to as ***fickle mining***.
  - – A miner chooses his coin as the easier one between two coins ***only when*** the coin mining difficulty changes.



Definition IV.1 (Fickle mining). *Let $D_{\mathtt{A}}$ and $D_{\mathtt{B}}$ denote the coin$_{\mathtt{A}}$ and coin$_{\mathtt{B}}$-mining difficulties, respectively. If $D_{\mathtt{B}} < \min\{r_{\mathcal{F}} + r_{\mathcal{B}}, k \cdot D_{\mathtt{A}}\}$ or $D_{\mathtt{B}} \leq r_{\mathcal{B}}$ when $D_{\mathtt{A}}$ or $D_{\mathtt{B}}$ is updated, fickle miners ($\mathcal{M}_{\mathcal{F}}$) decide to conduct coin$_{\mathtt{B}}$-mining until $D_{\mathtt{A}}$ or $D_{\mathtt{B}}$ is adjusted again. Otherwise, they conduct coin$_{\mathtt{A}}$-mining.*

Which equilibrium?
What change of hash rate?

Game analysis

- What does a *game* consist of?
  - Players: They act for a higher payoff (i.e., rationality).
  - Strategy: Any of the options which he or she chooses in a setting where the outcome depends *not only* on their own actions *but* on the actions of others.
  - Payoff: Depending on strategy of each player, they earn certain payoff.

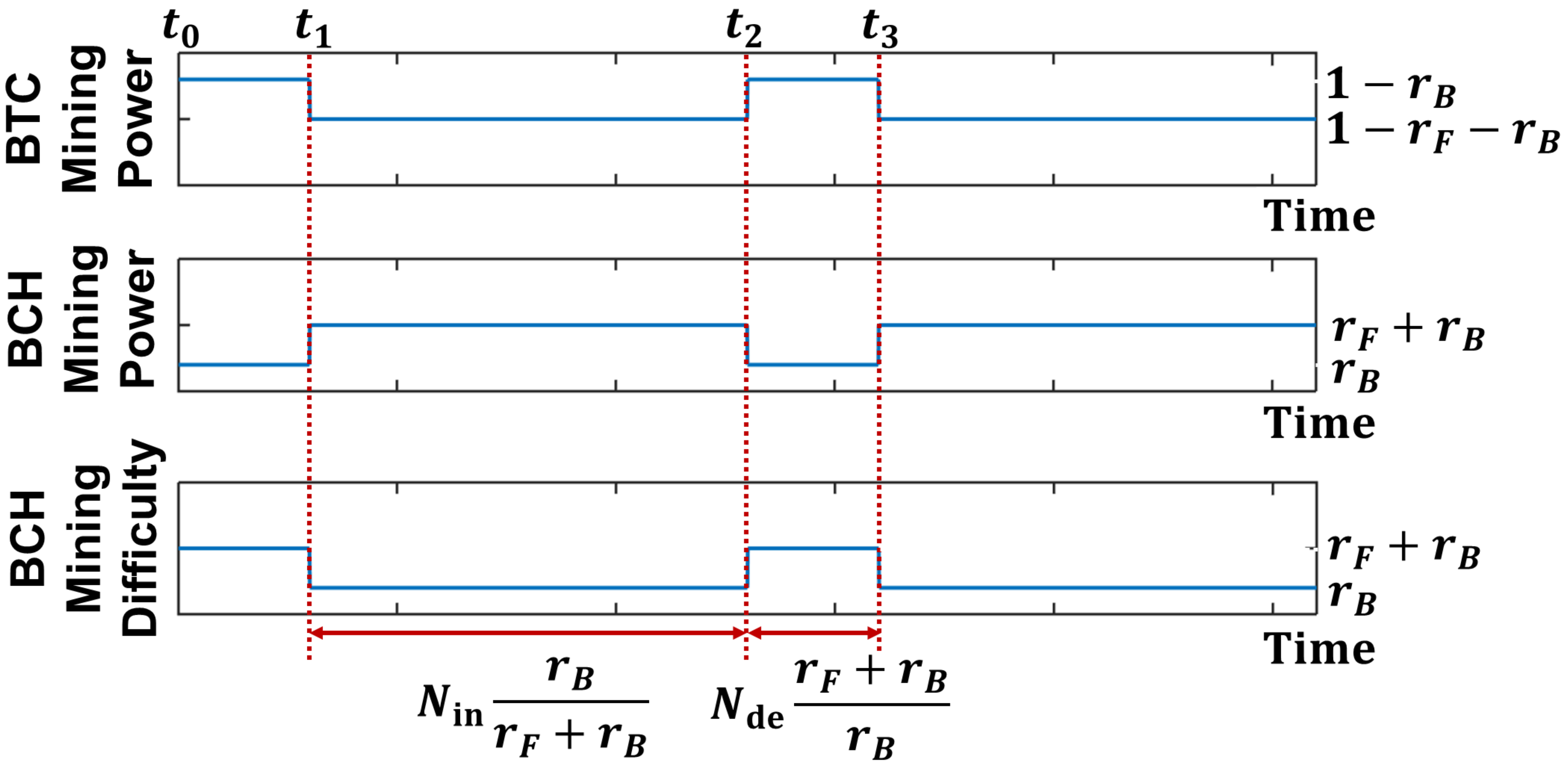
Game analysis

- What does a *game* consist of?
  - Players: Many miners with infinitesimal hash power

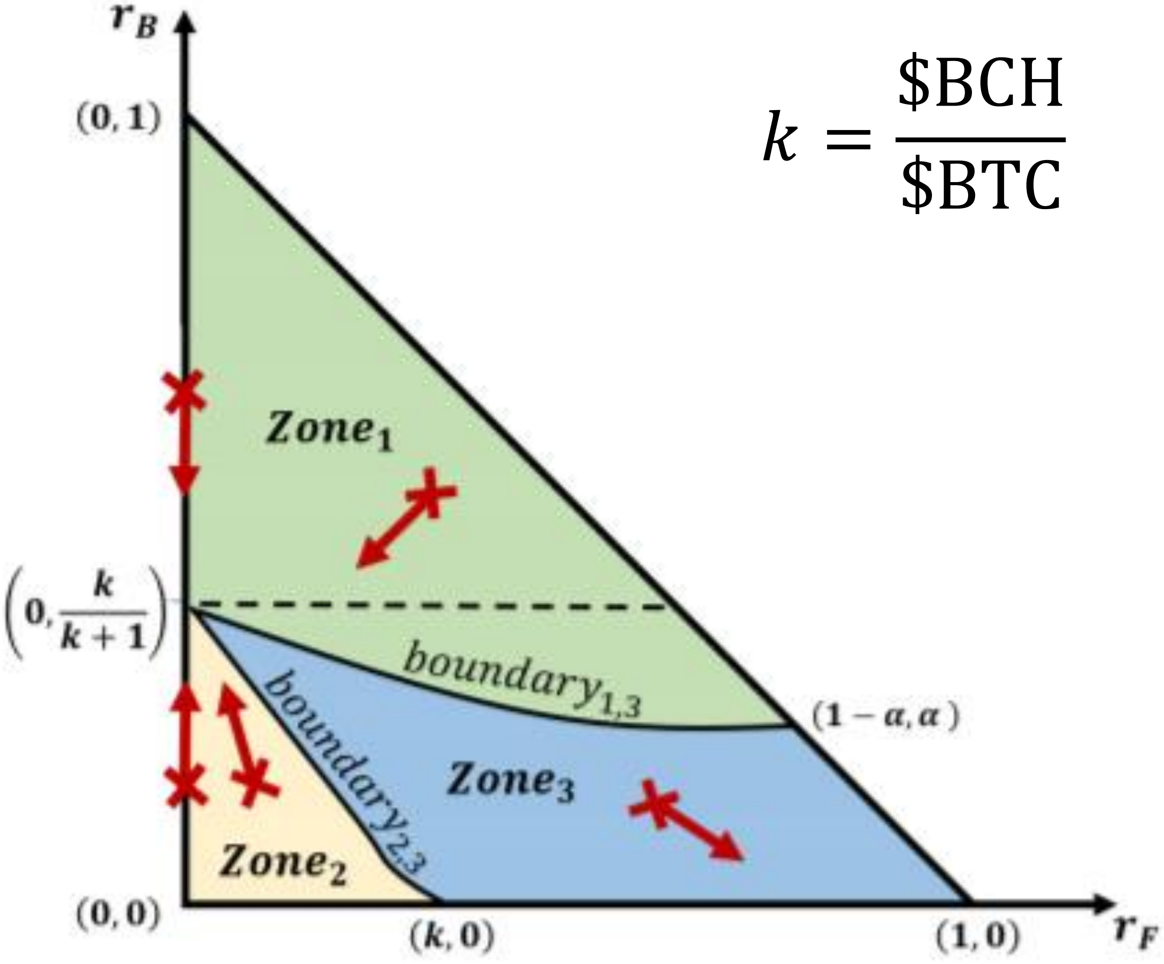
    Political BCH factions
  - Strategy: Fickle mining, only-BTC mining, only-BCH mining
  - Payoff:

$$U_i(s_i, \mathbf{s_{-i}}) = \begin{cases} U_{\mathcal{F}}(r_{\mathcal{F}}, r_{\mathcal{B}}) & \text{if the player chooses fickle mining} \\ U_{\mathcal{A}}(r_{\mathcal{F}}, r_{\mathcal{B}}) & \text{if the player chooses only BTC-mining} \\ U_{\mathcal{B}}(r_{\mathcal{F}}, r_{\mathcal{B}}) & \text{if the player chooses only BCH-mining} \end{cases}$$

Game analysis



Game analysis



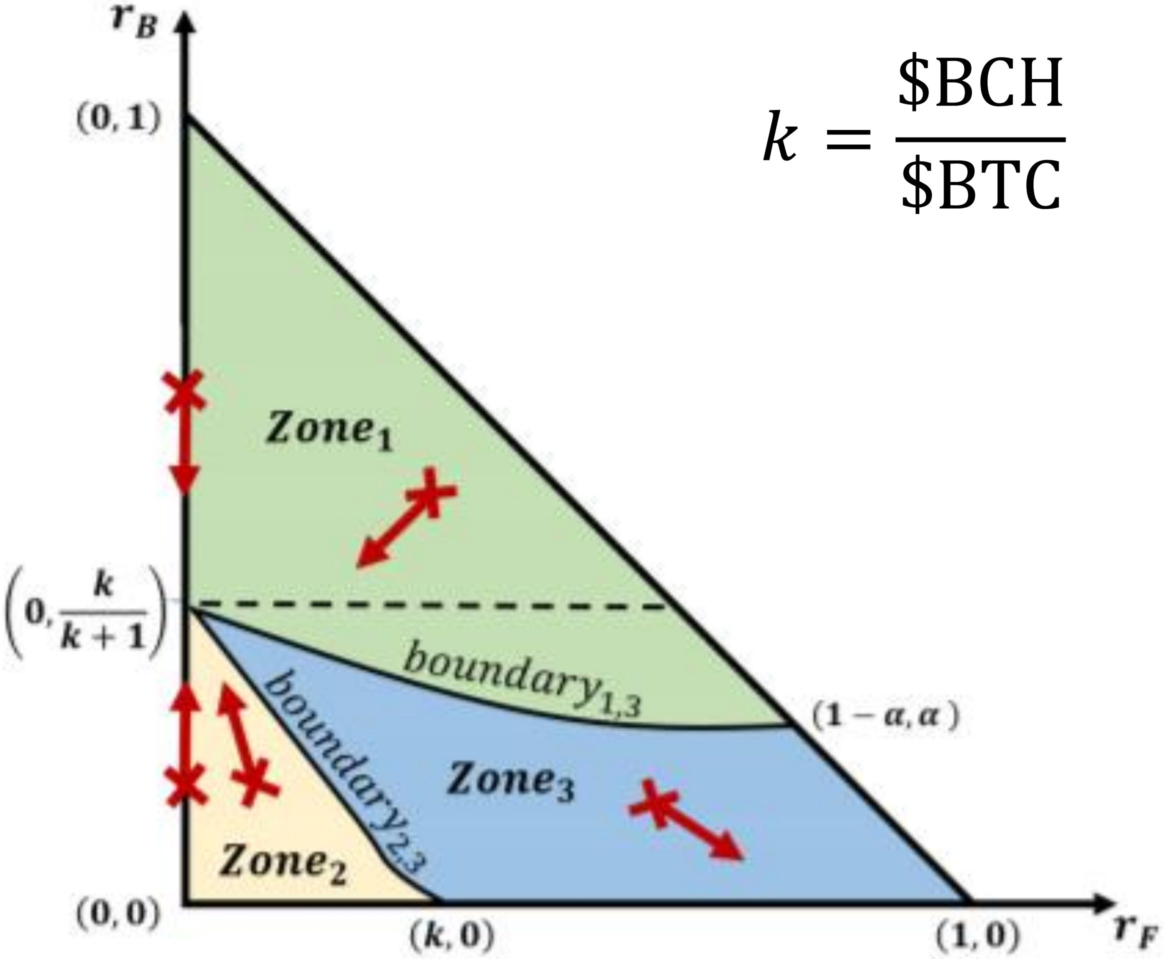
$$k = \frac{\$\text{BCH}}{\$\text{BTC}}$$

❖ $Zone_1$: It is most profitable to conduct only-BTC mining.

❖ $Zone_2$: It is most profitable to conduct only-BCH mining.

❖ $Zone_3$: It is most profitable to conduct fickle mining.

Game analysis

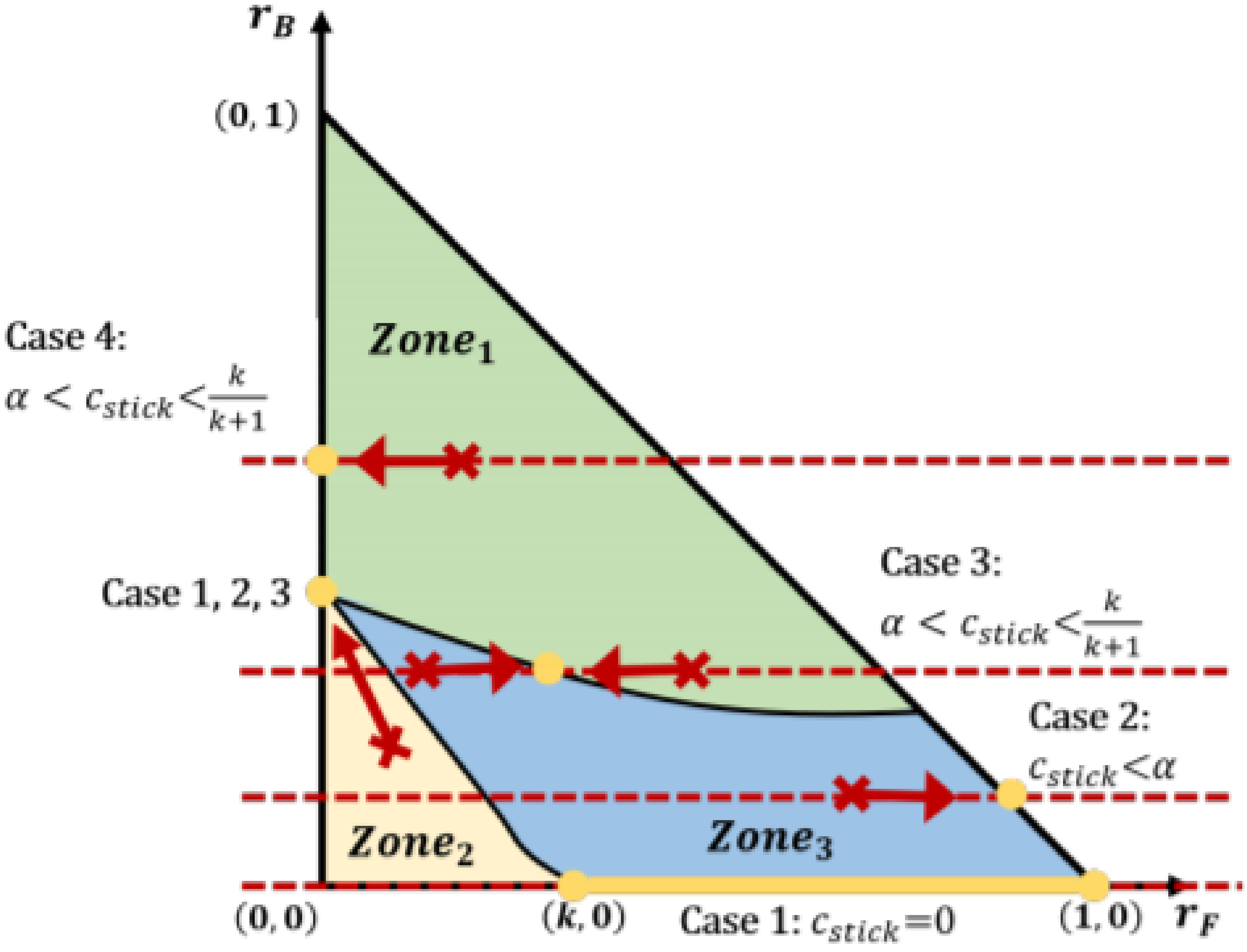


$$k = \frac{\$\mathrm{BCH}}{\$\mathrm{BTC}}$$

- $Zone_1$: It is most profitable to conduct only-BTC mining.
- $Zone_2$: It is most profitable to conduct only-BCH mining.
- $Zone_3$: It is most profitable to conduct fickle mining.

In each zone, a point moves along the corresponding arrow.

Game analysis



- There are two Nash equilibria: Coexistence and the lack of BCH loyal miners.

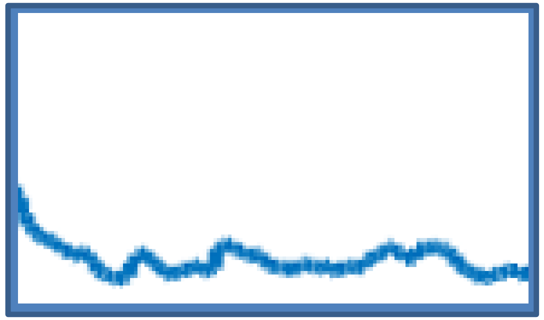
- If hash power sticking to BCH is large, there is only one Nash equilibria, the lack of BCH loyal miners.

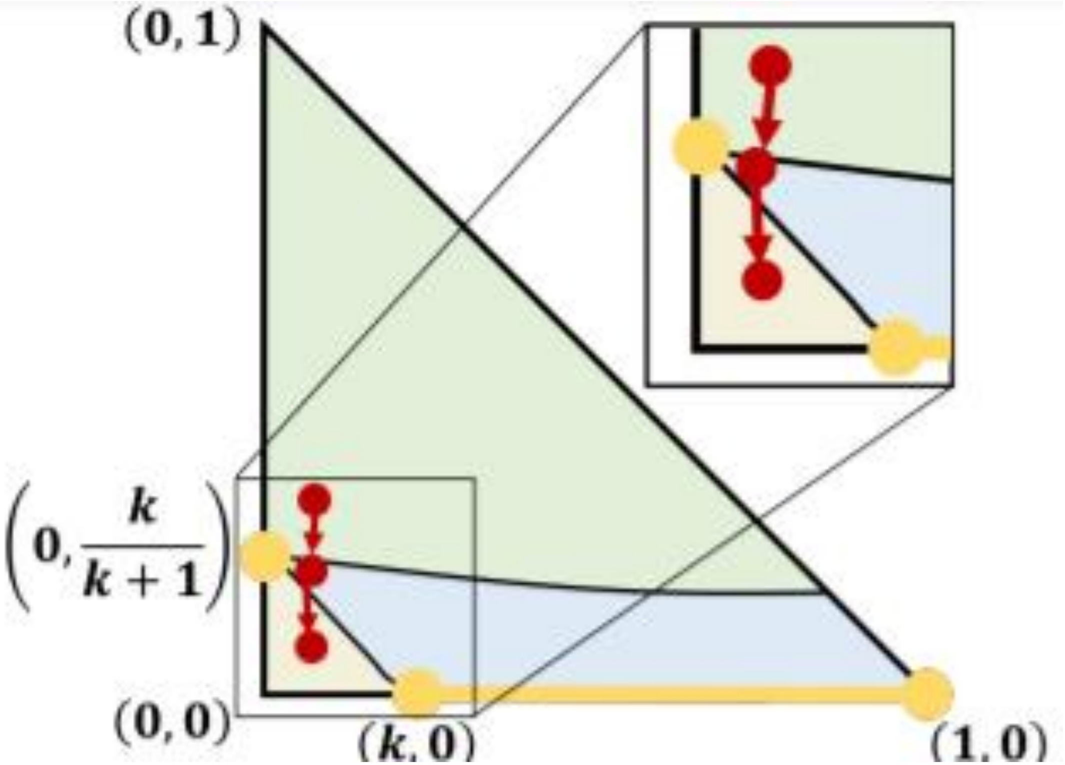
- If hash power sticking to BCH is zero, the lack of BCH loyal miners is equal to the complete downfall of BCH.

What happened in practice?

08/01/2017: Game start

Hash rate history

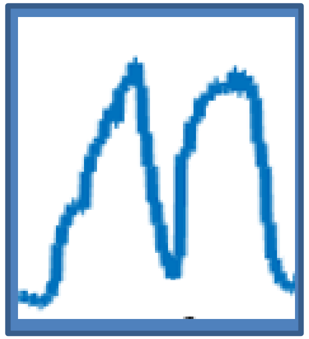


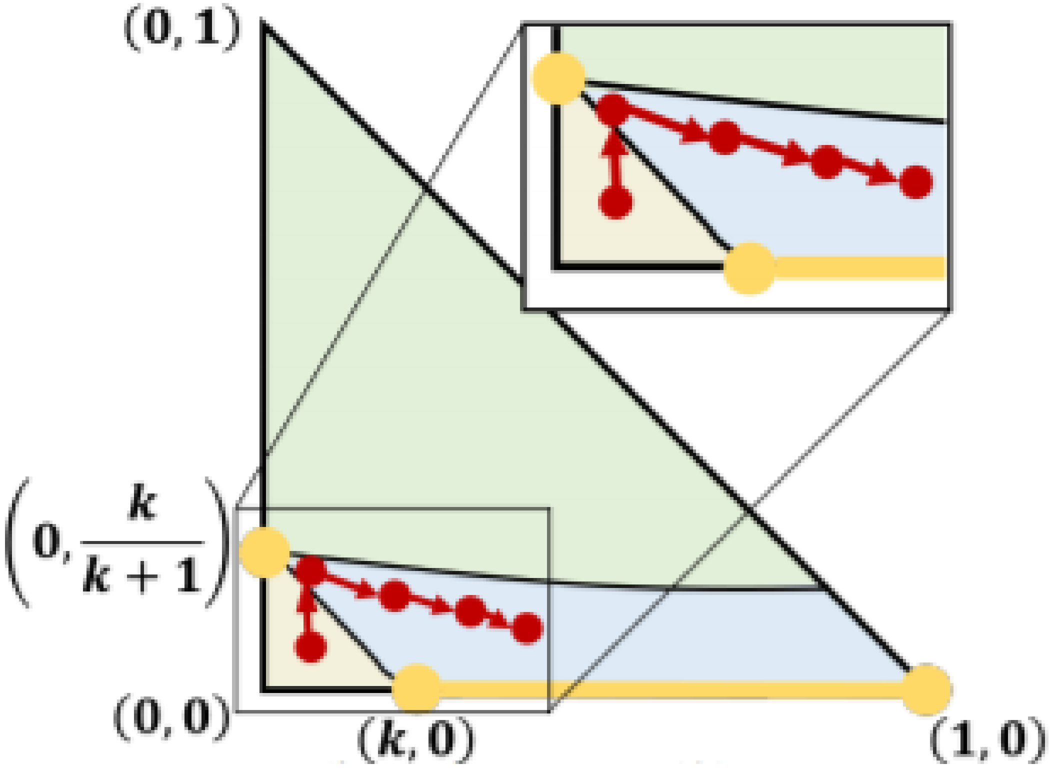


❖ The status point is initially in $Zone_1$, and then it moves to $Zone_2$.

Before 11/13/2017

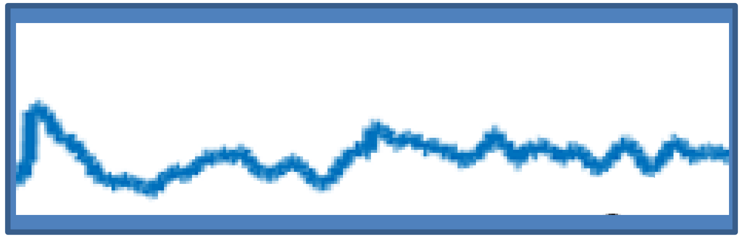
Hash rate history

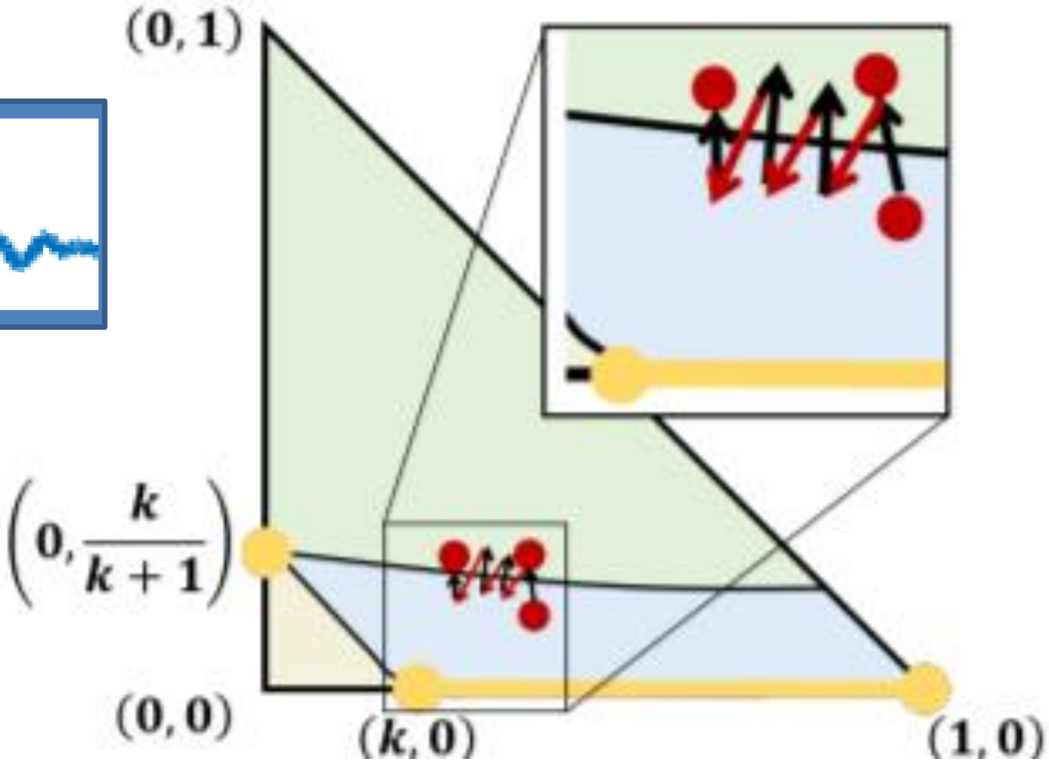




Before 11/13/2017

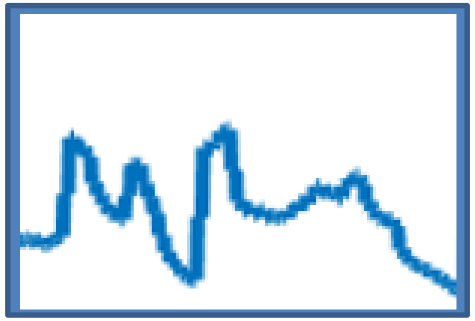
Hash rate history

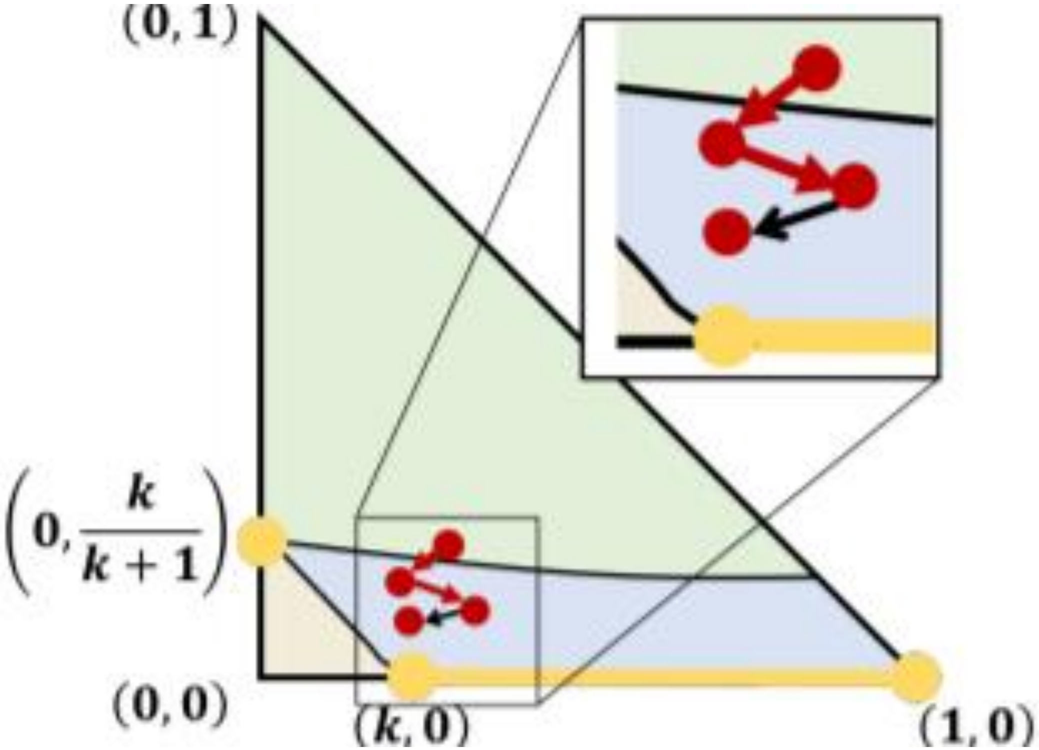




Before 11/13/2017

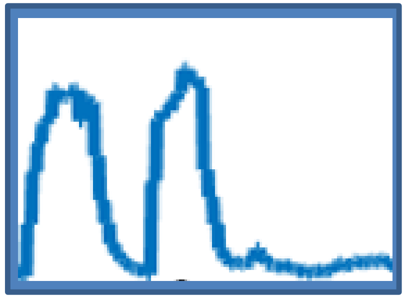
Hash rate history

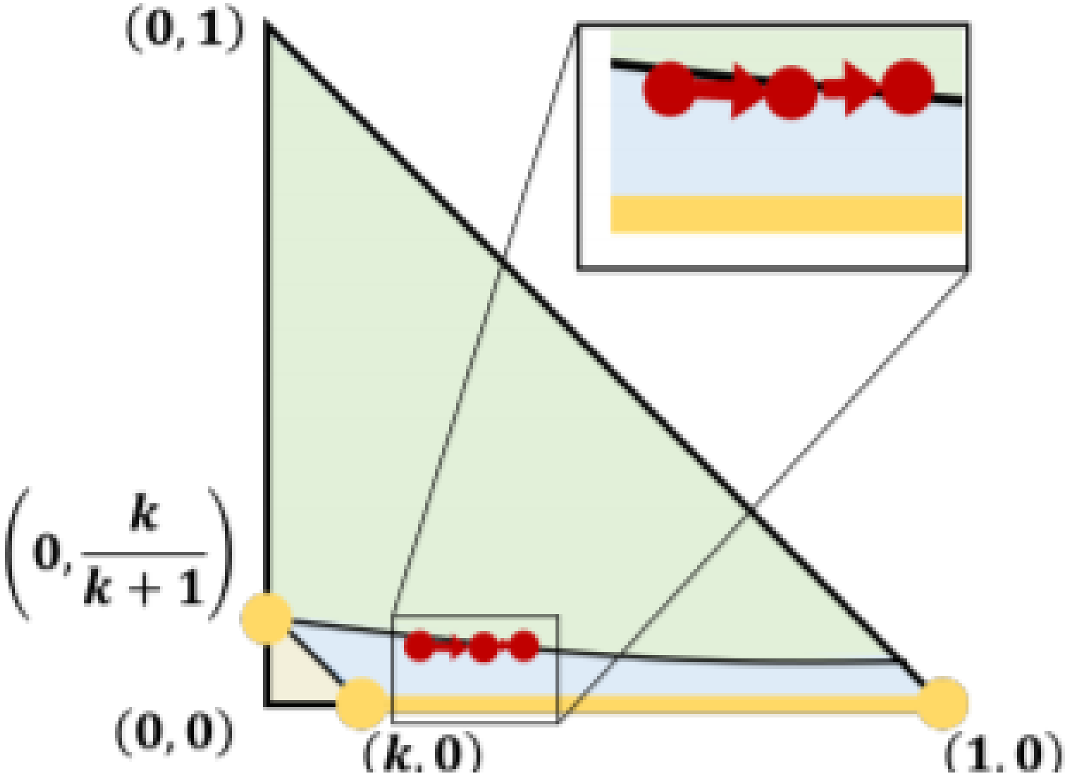




Before 11/13/2017

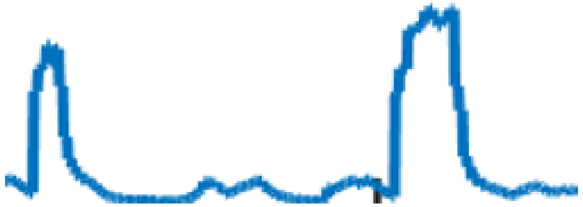
Hash rate history

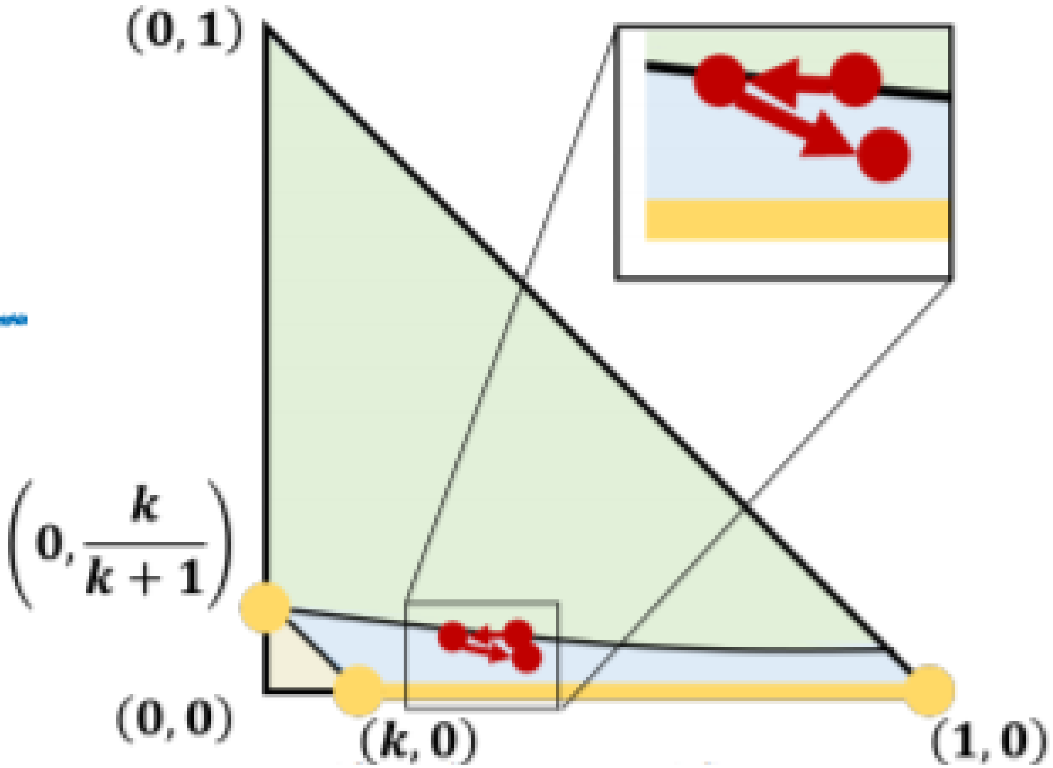




Before 11/13/2017

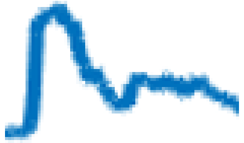
Hash rate history

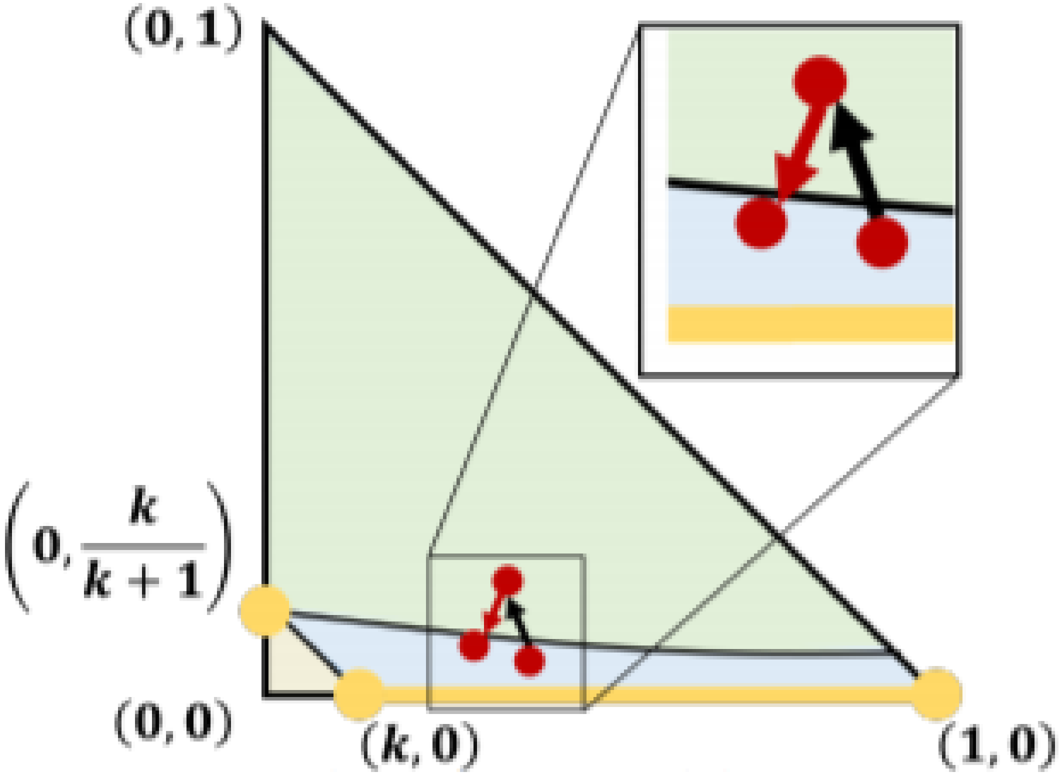




Before 11/13/2017

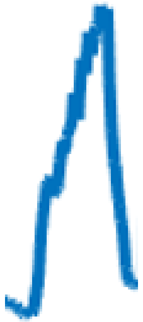
Hash rate history

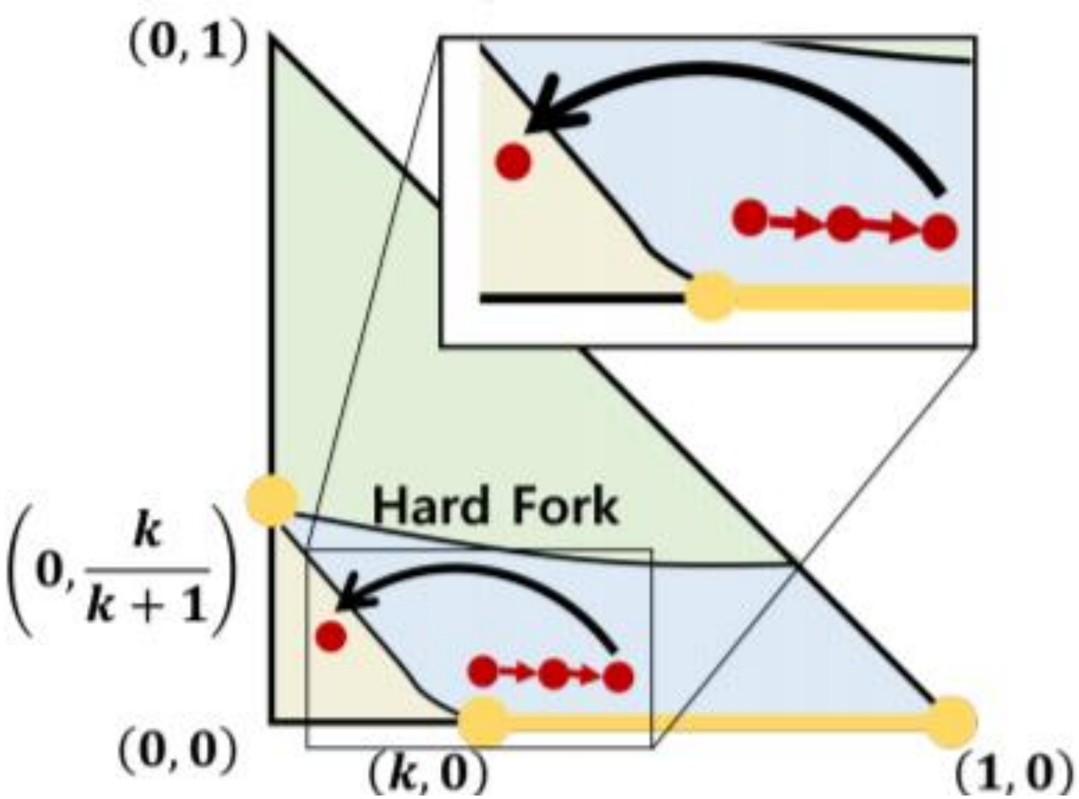




Before 11/13/2017

Hash rate history





The lack of BCH loyal miners

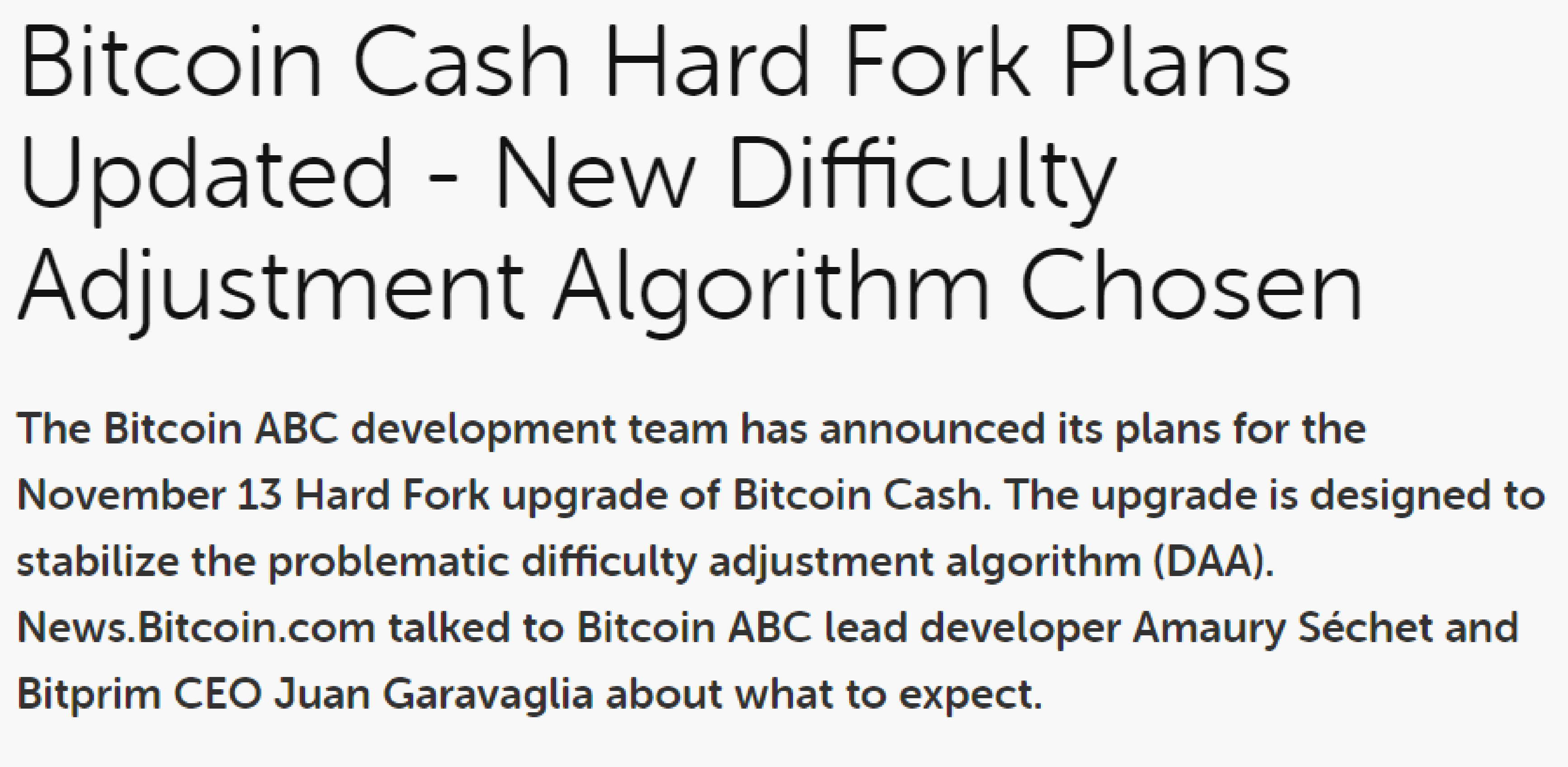
- The BCH transaction process speed periodically became low, and it even took about four hours to generate one block in some cases.
- From Oct. 2 to Oct. 4, Only two accounts generated about 70 % of blocks and there were only five miners who conducted BCH mining.
- BCH before Nov. 13, 2017 was susceptible to double spending attacks with only 1～2% of the total computational power in the Bitcoin system.

The lack of BCH loyal miners

- The BCH transaction process speed periodically became low, and it even took about four hours to generate one block in some cases.
- From Oct. 2 to Oct. 4, Only two accounts generated about 70 % of blocks and there were only five miners who conducted BCH mining.
- BCH before Nov. 13, 2017 was susceptible to double spending attacks with only 1～2% of the total computational power in the Bitcoin system.

Both Scalability, Decentralization, and Security are undermined!

On 11/13/2017: Hard fork



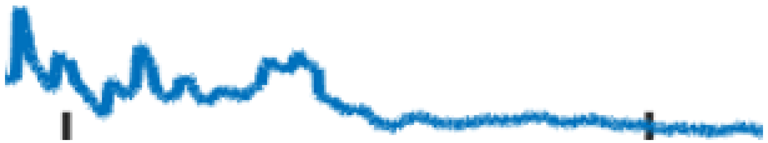
Bitcoin Cash Hard Fork Plans Updated - New Difficulty Adjustment Algorithm Chosen

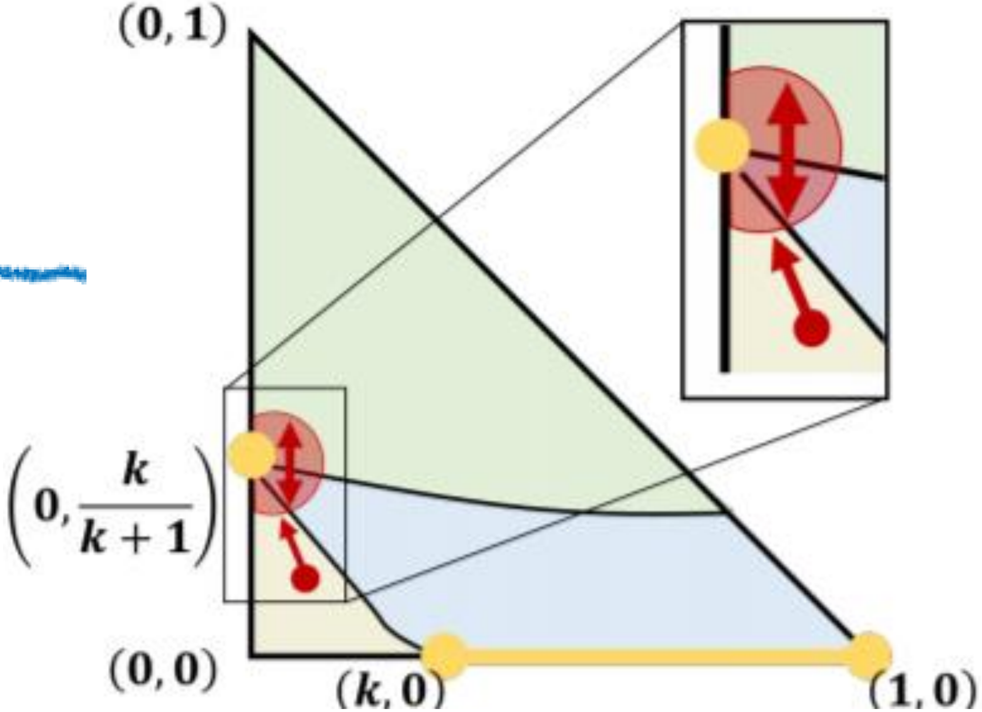
The Bitcoin ABC development team has announced its plans for the November 13 Hard Fork upgrade of Bitcoin Cash. The upgrade is designed to stabilize the problematic difficulty adjustment algorithm (DAA). News.Bitcoin.com talked to Bitcoin ABC lead developer Amaury Séchet and Bitprim CEO Juan Garavaglia about what to expect.

- BCH updates its mining difficulty adjustment algorithm.
- This change affected the game as an external factor.

After 11/13/2017

Hash rate history



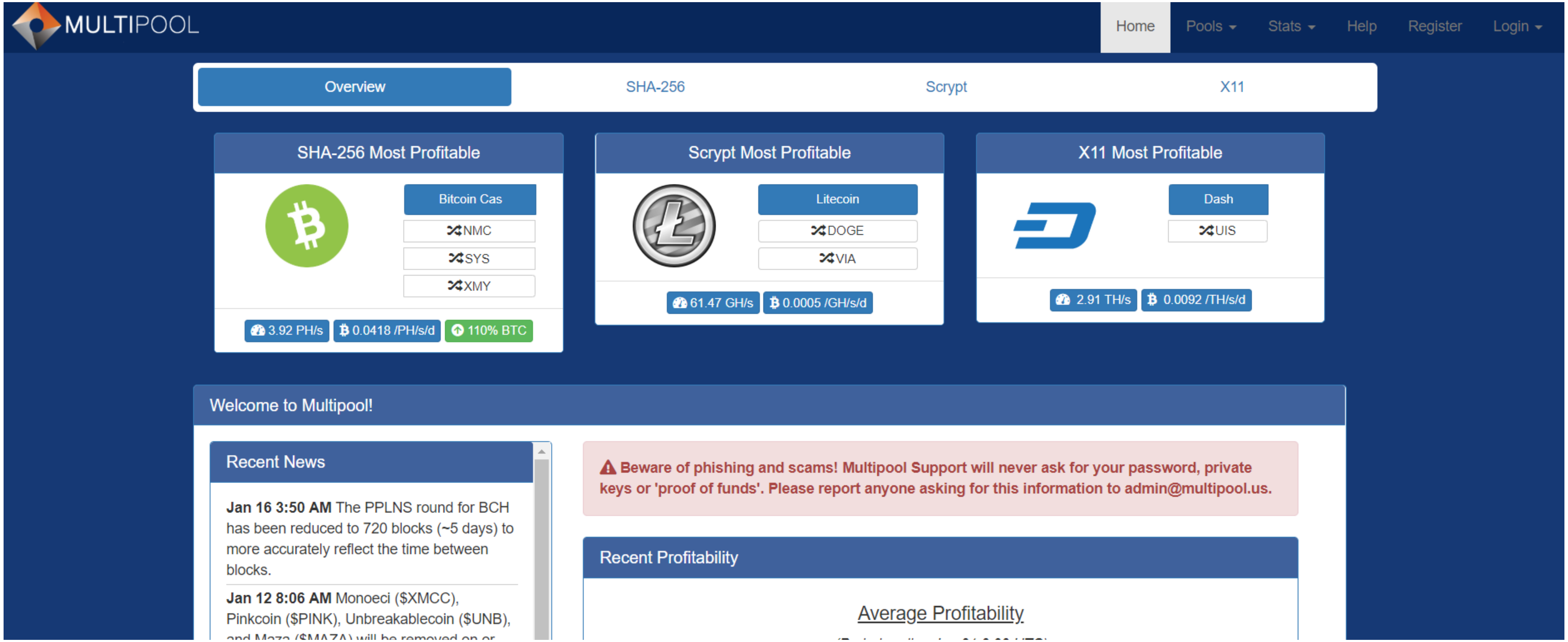


❖ The status point gradually became close to the coexistence.

Now BCH is safe?

Automatic mining

- ❖ Miners can automatically choose the most profitable coin.



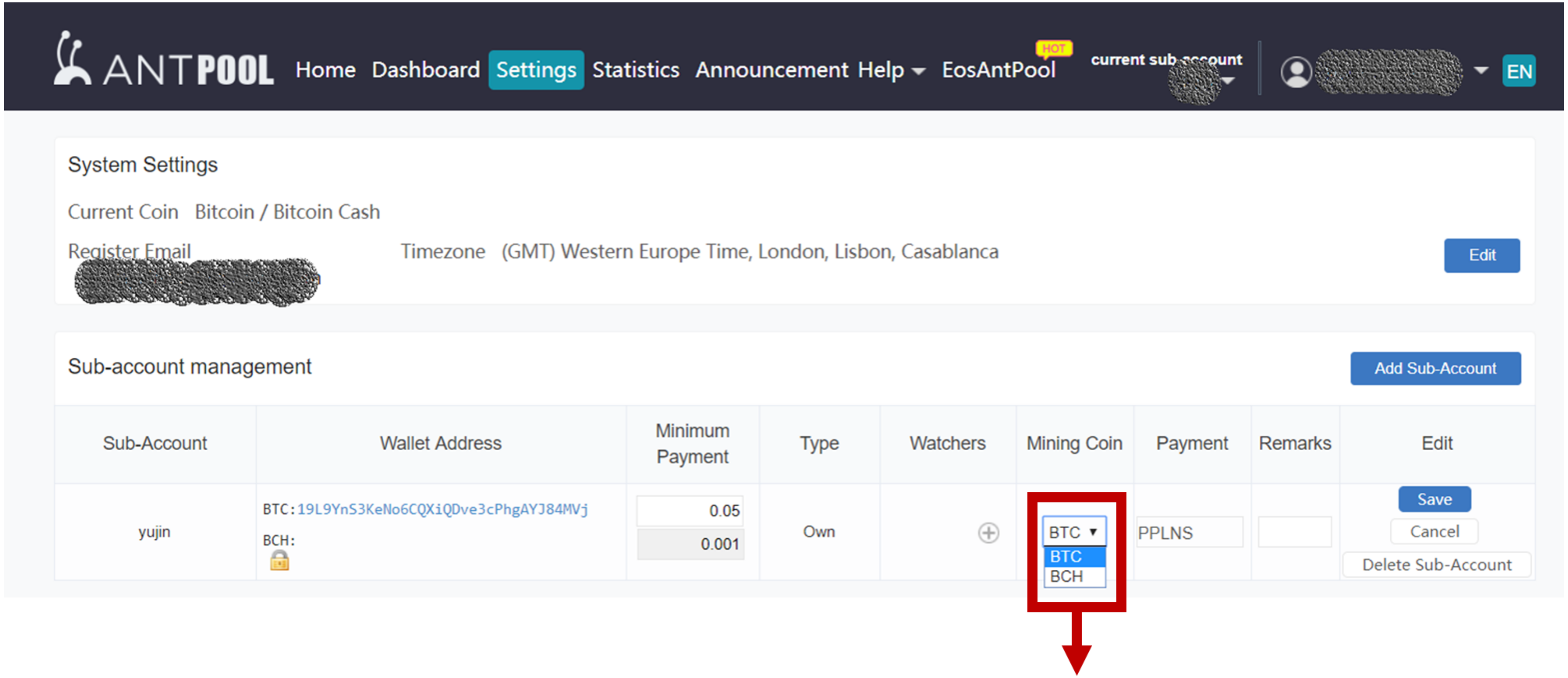
Jan 16 3:50 AM The PPLNS round for BCH has been reduced to 720 blocks (~5 days) to more accurately reflect the time between blocks.

Jan 12 8:06 AM Monoeci ($XMCC), Pinkcoin ($PINK), Unbreakablecoin ($UNB), and Maza ($MAZA) will be removed on or

⚠ Beware of phishing and scams! Multipool Support will never ask for your password, private keys or 'proof of funds'. Please report anyone asking for this information to admin@multipool.us.

Automatic mining

- ❖ Miners can automatically choose the most profitable coin.



System Settings

Current Coin Bitcoin / Bitcoin Cash

Register Email [redacted] Timezone (GMT) Western Europe Time, London, Lisbon, Casablanca

Sub-account management

Sub-Account	Wallet Address	Minimum Payment	Type	Watchers	Mining Coin	Payment	Remarks	Edit
yujin	BTC:19L9YnS3KeNo6CQXiQDve3cPhgAYJ84MVj BCH: 🔒	0.05 0.001	Own	⊕	BTC ▾ BTC BCH	PPLNS		Save Cancel Delete Sub-Account

One-button switch

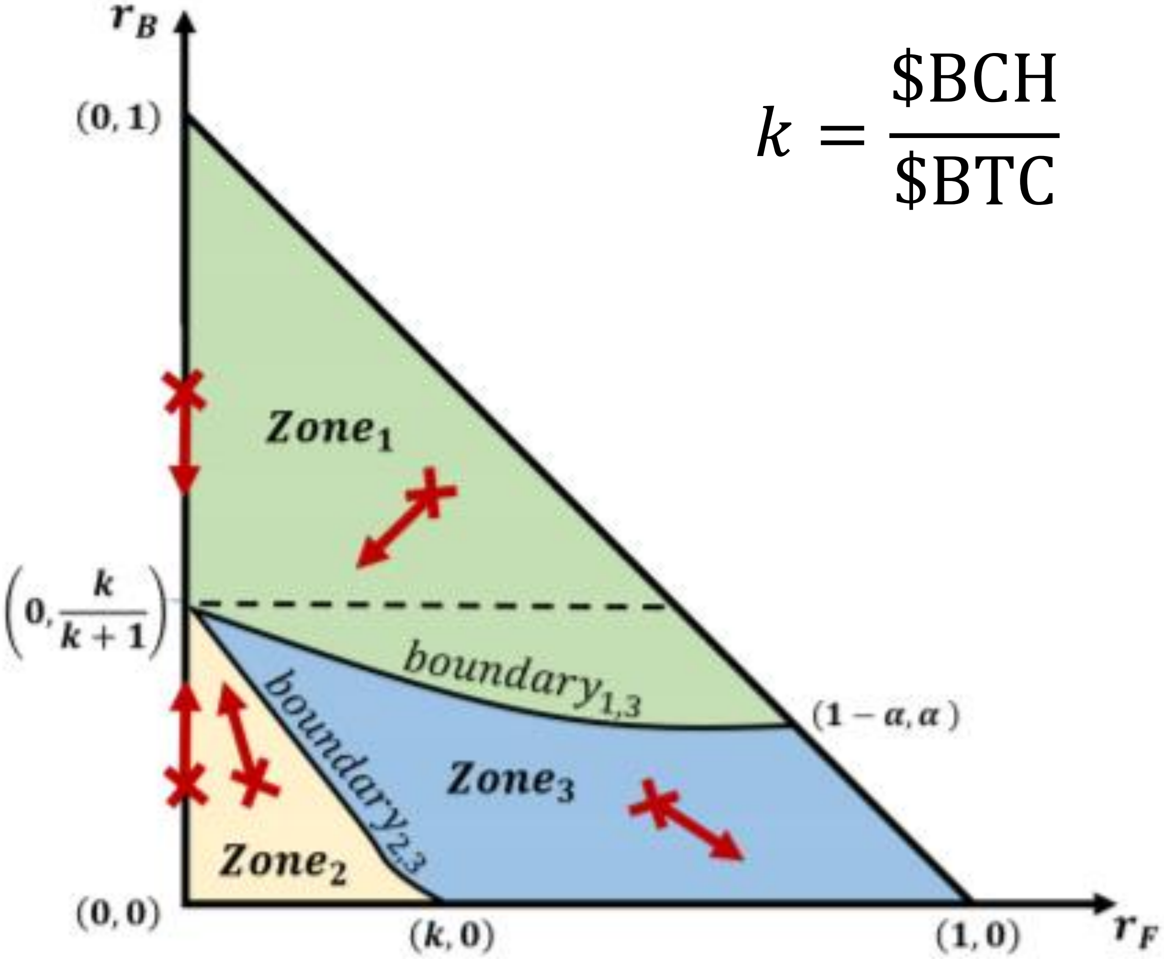
Automatic mining

- Miners can automatically choose the most profitable coin.

- They switch their coin almost ***simultaneously*** both when the coin price changes and when the coin mining difficulty changes.

- This can be considered to be automatically choosing the most profitable one among three strategies, (fickle mining, only-BTC mining, only-BCH mining) in real time.

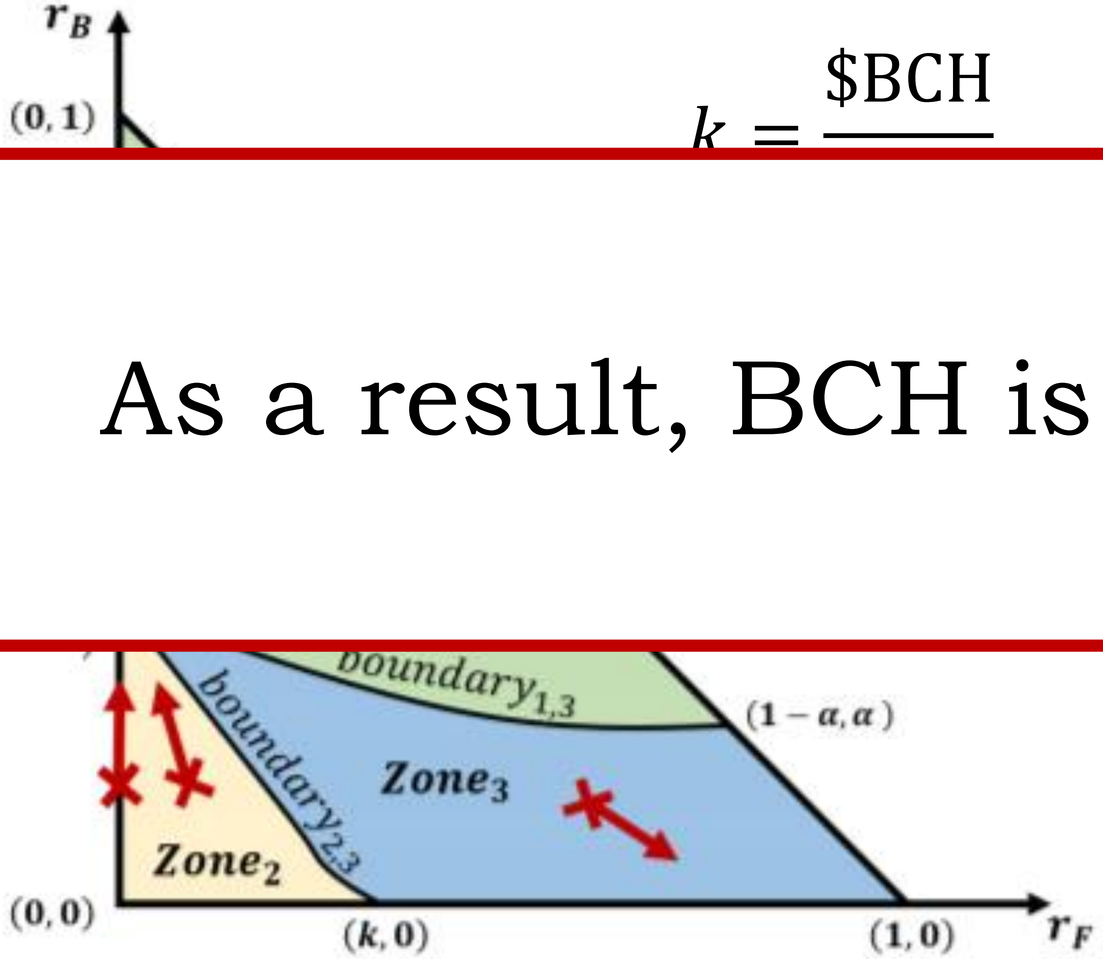
Automatic mining



$$k = \frac{\$\text{BCH}}{\$\text{BTC}}$$

- When a fraction k of the total mining power is involved in the automatic fickle mining, the state moves towards a lack of BCH-loyal miners.

Automatic mining



$$k = \frac{\$\text{BCH}}{}$$

er

k

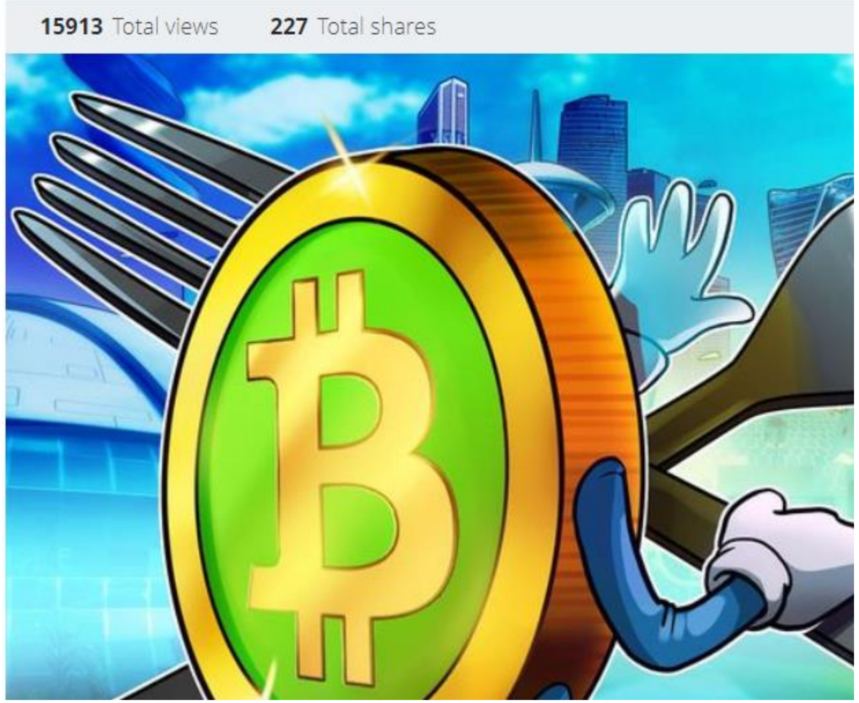
of BCH-loyal miners.

As a result, BCH is still not safe.

Bitcoin ABC vs. Bitcoin SV: Hash war

Bitcoin ABC vs. Bitcoin SV

Opposing Bitcoin ABC and Bitcoin SV Factions’ Debates Grow Heated as the Bitcoin Cash Hard Fork Draws Closer

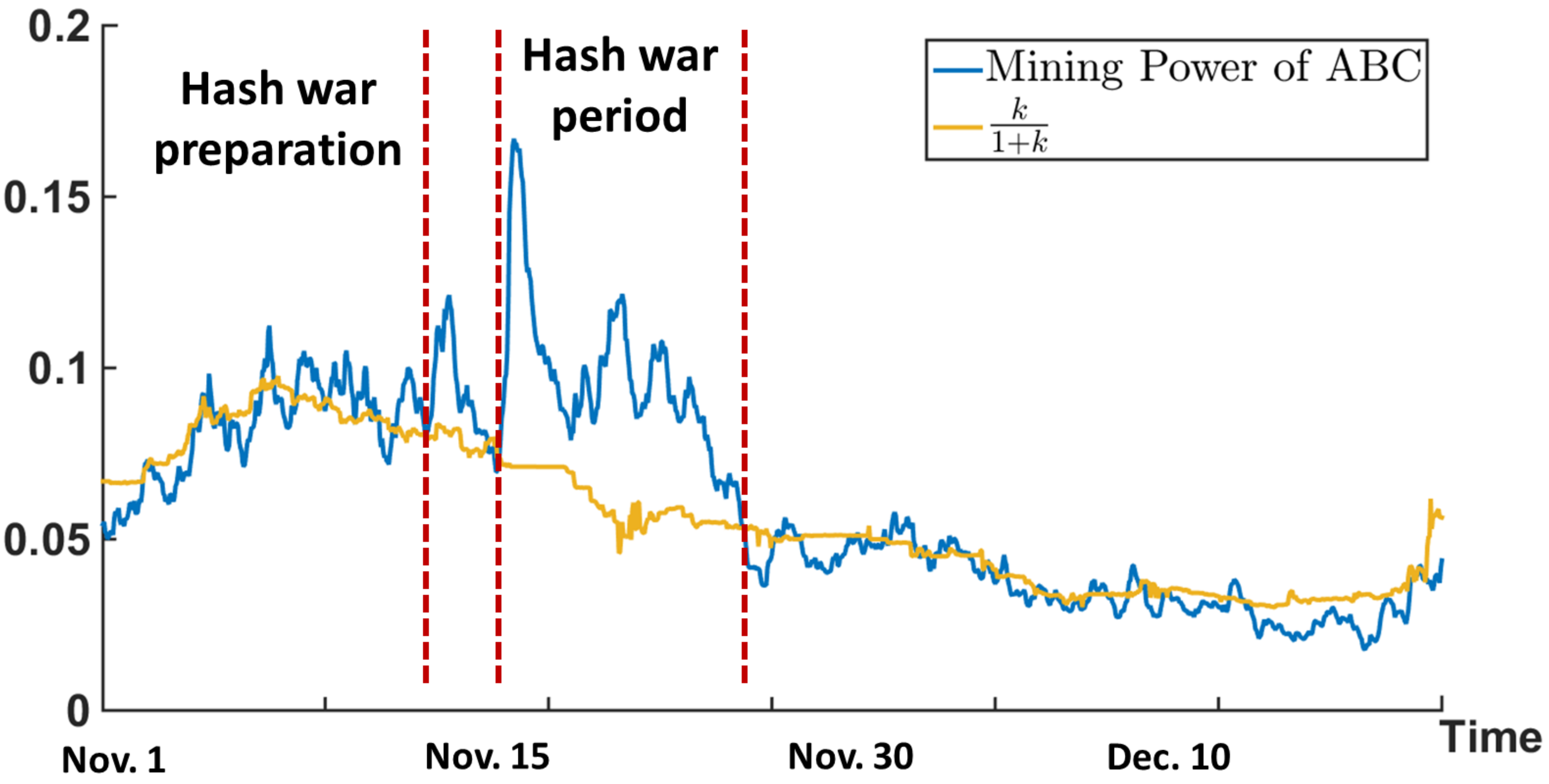


15913 Total views **227** Total shares

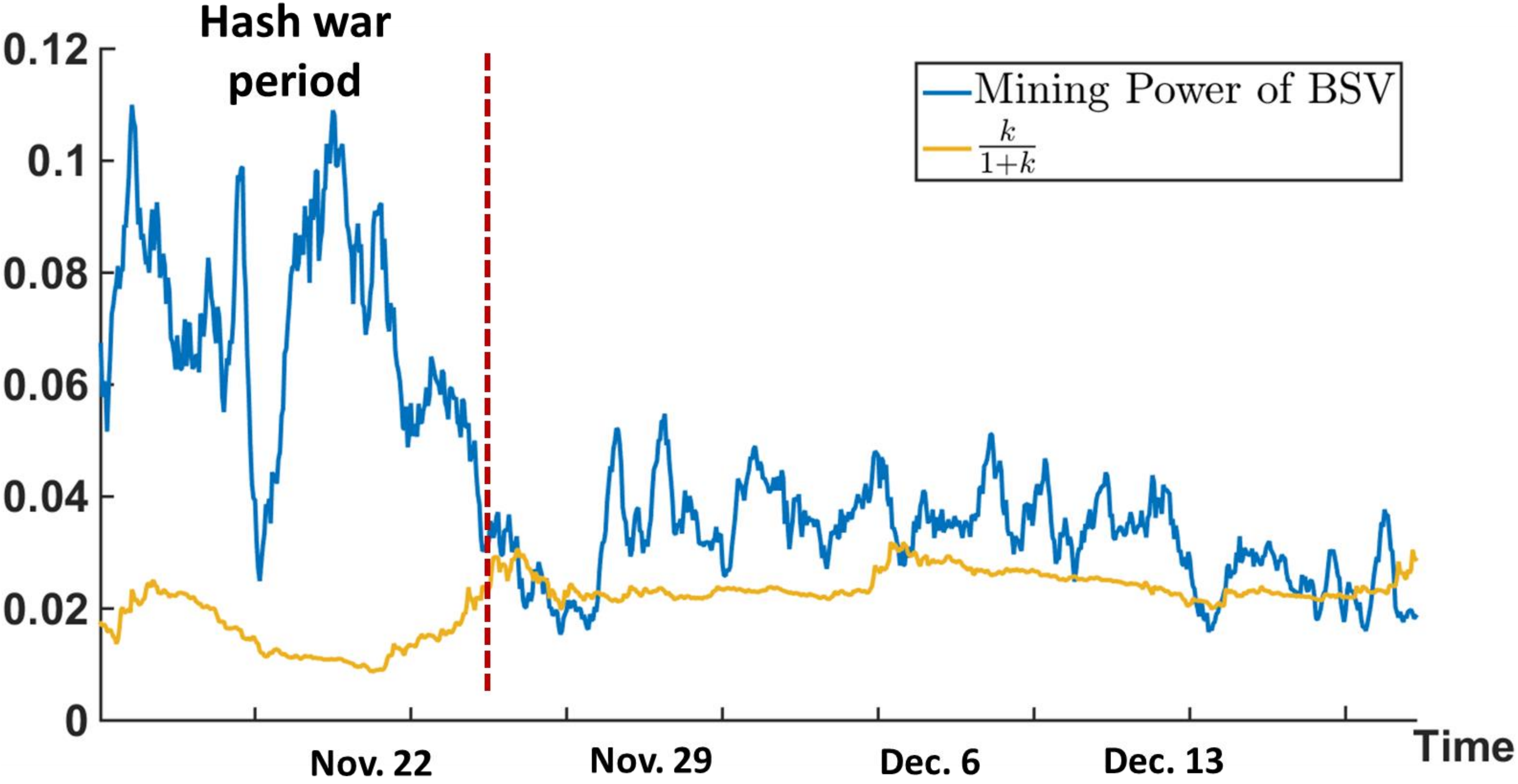
Bitcoin Cash Fork Race: Bad News to the Faketoshi Team

By **Fredrik Vold** • November 09, 2018

Bitcoin ABC vs. Bitcoin SV

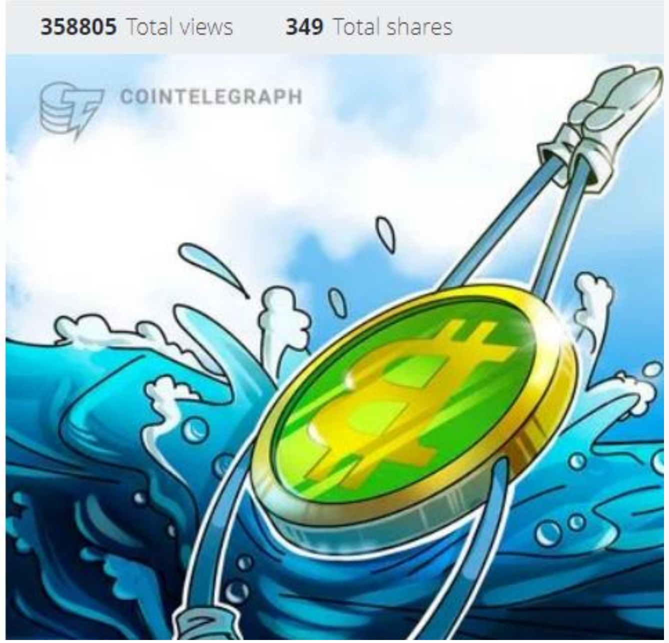


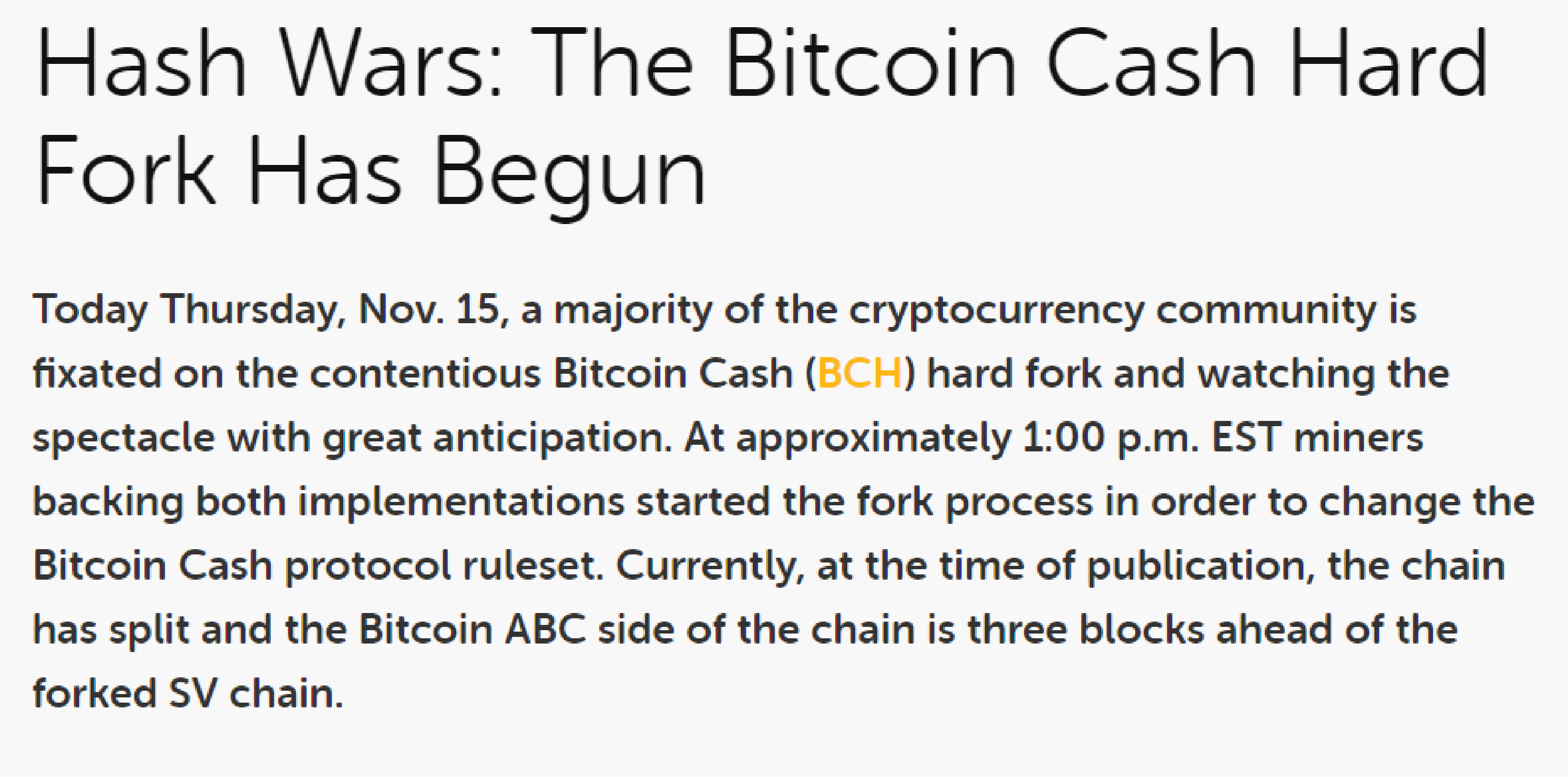
Bitcoin ABC vs. Bitcoin SV



Hash war

Bitcoin Cash Hard Fork Battle: Who Is Winning the Hash War


358805 Total views 349 Total shares

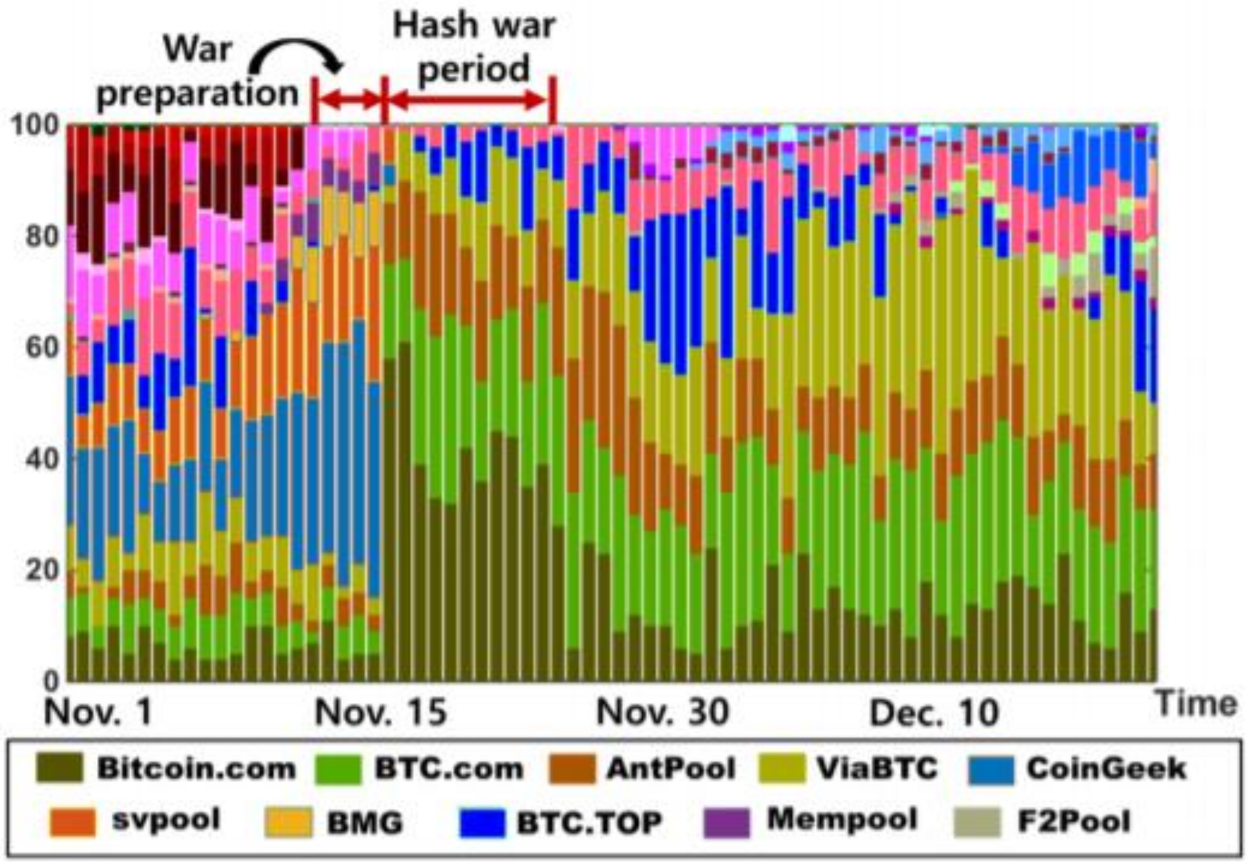


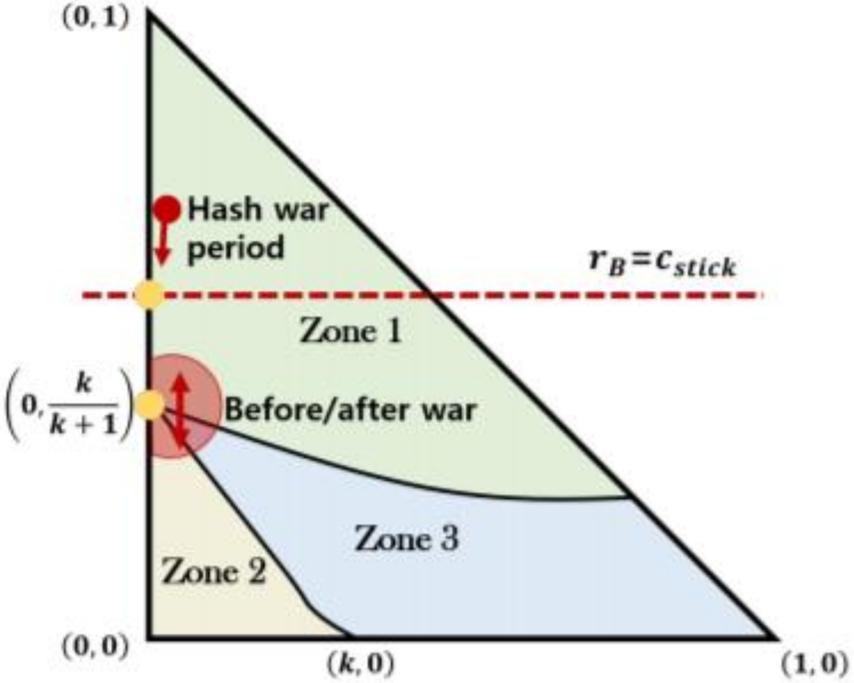
Hash Wars: The Bitcoin Cash Hard Fork Has Begun

Today Thursday, Nov. 15, a majority of the cryptocurrency community is fixated on the contentious Bitcoin Cash (BCH) hard fork and watching the spectacle with great anticipation. At approximately 1:00 p.m. EST miners backing both implementations started the fork process in order to change the Bitcoin Cash protocol ruleset. Currently, at the time of publication, the chain has split and the Bitcoin ABC side of the chain is three blocks ahead of the forked SV chain.

Hash war

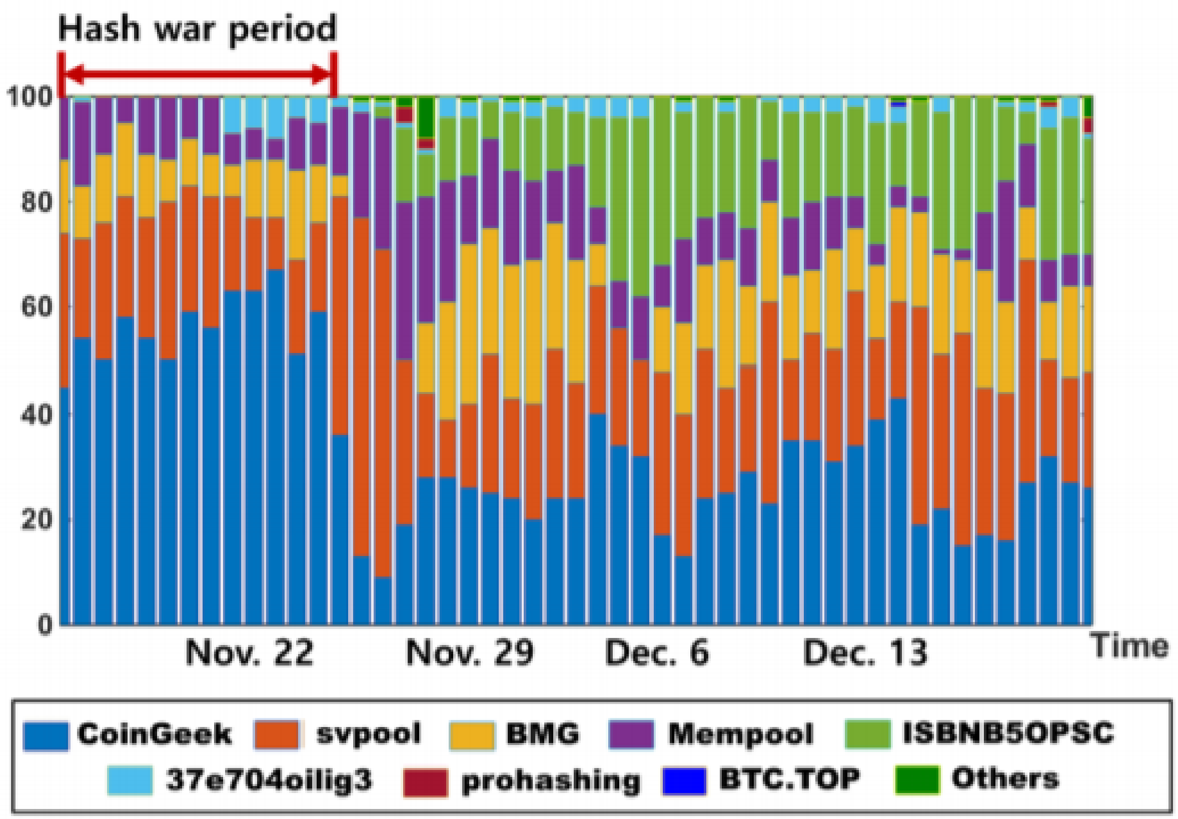
- Bitcoin ABC hash rate distribution

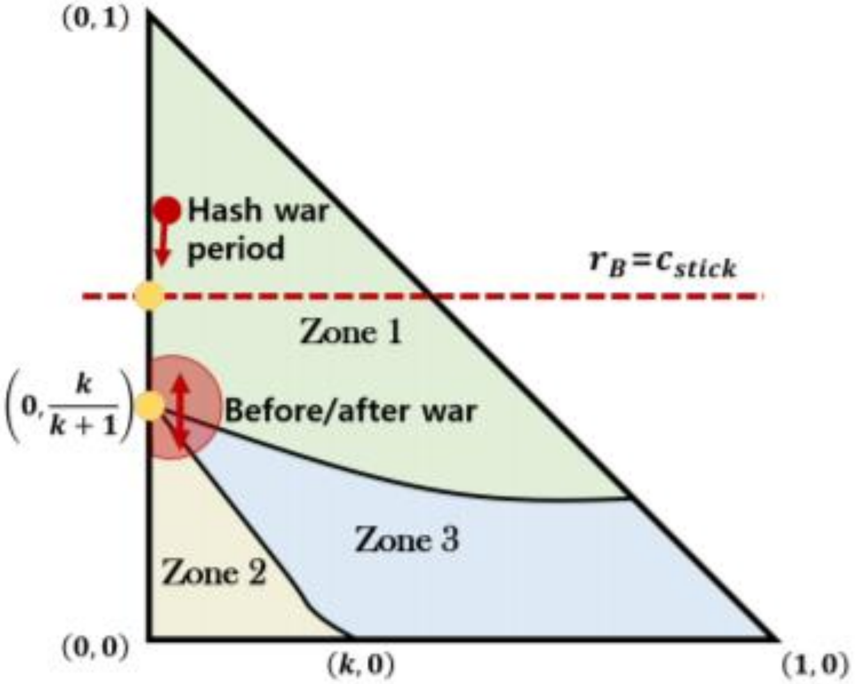




Hash war

- Bitcoin SV hash rate distribution





Conclusion

- Fickle mining leads to a lack of loyal miners.
  - There are two Nash equilibria: Coexistence and downfall of BCH.

- Automatic mining is also dangerous.
  - When a fraction k of the total mining power is involved in the automatic fickle mining, the state moves towards a lack of BCH-loyal miners.

Thank you!