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

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

*KAIST, ° Sungkyunkwan University
Governance conflict

The number of Bitcoin transaction per month

Bad scalability
Several solutions were proposed.
Governance conflict

The number of Bitcoin transaction per month

Due to political conflict, Bitcoin was 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 do 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 Bitcoin (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.
When the BCH mining difficulty becomes easy, large hash power moves from BTC to BCH.
Fickle mining

- The following behavior 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.
Equilibrium in this situation?
Change of mining power?
What is your choice?

- Players: **Many miners with small hash power**
  - Political BCH factions (e.g., BITMAIN)

A normal miner

- Fickle mining
- Only-BTC mining
- Only-BCH mining
What is your choice?

- Players: Many miners with small hash power
  - Political BCH factions (e.g., BITMAIN)

I should maintain BCH!
Coexistence or downfall of BCH?

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

Hash power ratio of only-BCH mining

Hash power ratio of fickle mining
Coexistence or downfall of BCH?

$ 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.
Coexistence or downfall of BCH?

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

Hash power ratio of only-BCH mining

Hash power ratio of fickle mining

$k = \frac{BCH}{BTC}$
Coexistence or downfall of BCH?

1) When the hash power ratio of political BCH factions is 0.
Coexistence or downfall of BCH?

2) When the hash power ratio of political BCH factions is small

A lack of BCH loyal miners

Hash power ratio of BCH factions

Coexistence
Coexistence or downfall of BCH?

3) When the hash power ratio of political BCH factions is not small

A lack of BCH loyal miners

Hash power ratio of BCH factions

Coexistence

$k = \frac{BCH}{BTC}$
Coexistence or downfall of BCH?

A lack of BCH loyal miners

Hash power ratio of BCH factions

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

4) When the hash power ratio of political BCH factions is large
What happened in practice?
08/01/2017: Game start

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

...
The lack of BCH loyal miners

- **Scalability:**
  - The BCH transaction process speed periodically became low
  - even took **four hours** to generate one block in some cases.

- **Decentralization:**
  - Only **two accounts** generated about 70% of blocks
  - There were only **five miners**

- **Security:**
  - Susceptible to double spending attacks with only **1~2%** of the total computational power
The lack of BCH loyal miners

- **Scalability:**
  - The BCH transaction process speed periodically became low
  - Even took four hours to generate one block in some cases.

- **Decentralization:**
  - Only two accounts generated about 70% of blocks
  - There were only five miners

- **Security:**
  - Susceptible to double spending attacks with only 1~2% of the total computational power

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.
On 11/13/2017: Hard fork

- BCH updates its mining difficulty adjustment algorithm.
- This change affected the game as an external factor.
After 11/13/2017

The status point gradually became close to the coexistence.
Now BCH is safe?
Automatic mining

- Miners can automatically choose the most profitable coin.
Automatic mining

- Miners can automatically choose the most profitable coin.
Automatic mining

- **When the coin price or mining difficulty** changes, miners can immediately switch the coin to be mined.

![Diagram](image.png)

- **Bitcoin (BTC)**
- **Bitcoin Cash (BCH)**
Fickle mining

- Only when **mining difficulty** changes, miners can immediately switch the coin to be mined.

Bitcoin (BTC)  

Bitcoin Cash (BCH)
Automatic mining

- When the coin price or mining difficulty changes, miners can immediately switch the coin to be mined.

This can be considered to be automatically choosing the most profitable one among fickle mining, only-BTC mining, and only-BCH mining in real time.
When a ratio $k$ (5%) of the total mining power is involved in the automatic fickle mining, the state moves towards a lack of BCH-loyal miners.
When a ratio $k$ (5 %) of the total mining power is involved in the automatic mining, the state moves towards a lack of BCH-loyal miners.
When a fraction $k$ of the total mining power is involved in the automatic mining, the state moves towards a lack of BCH-loyal miners. As a result, BCH is still not safe, when 5% of hash power is involved in automatic mining.

$k = \frac{\text{BCH}}{\text{BTC}}$
Bitcoin ABC vs. Bitcoin SV: Hash war
Coexistence or downfall of BCH?

4) When the hash power ratio of political BCH factions is large.

A lack of BCH loyal miners

Hash power ratio of BCH factions
Ethereum vs. Ethereum Classic?
Generalization

- Our analysis can be applied to any two coins that have compatible mining algorithms.

- Major coin should have a mining difficulty algorithm similar to Bitcoin.
Generalization

- Our analysis can be applied in any two coins that have compatible mining algorithms.

- Major coin should have a similar mining difficulty algorithm to Bitcoin.

- Ethereum can undermine Ethereum classic through the mining difficulty adjustment algorithm update.
Conclusion

- Through fickle mining and automatic mining, one major coin can undermine the health of minor coin systems.
Thank you!