

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

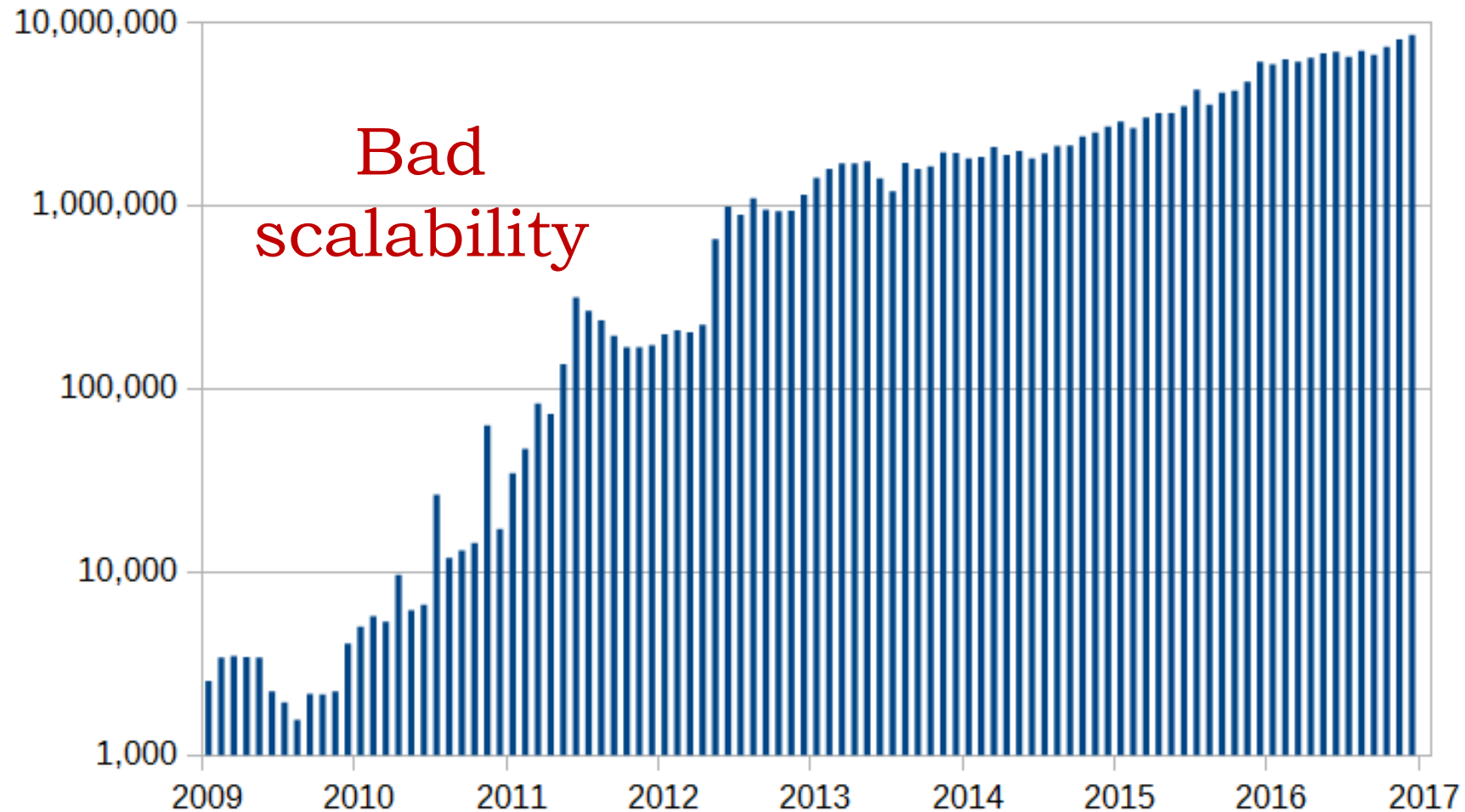
**Yujin Kwon\***, Hyoungshick Kim<sup>°</sup>, Jinwoo Shin\*, Yongdae Kim\*

\*KAIST, <sup>°</sup> Sungkyunkwan University

# Governance conflict

---

**The number of Bitcoin transaction per month**



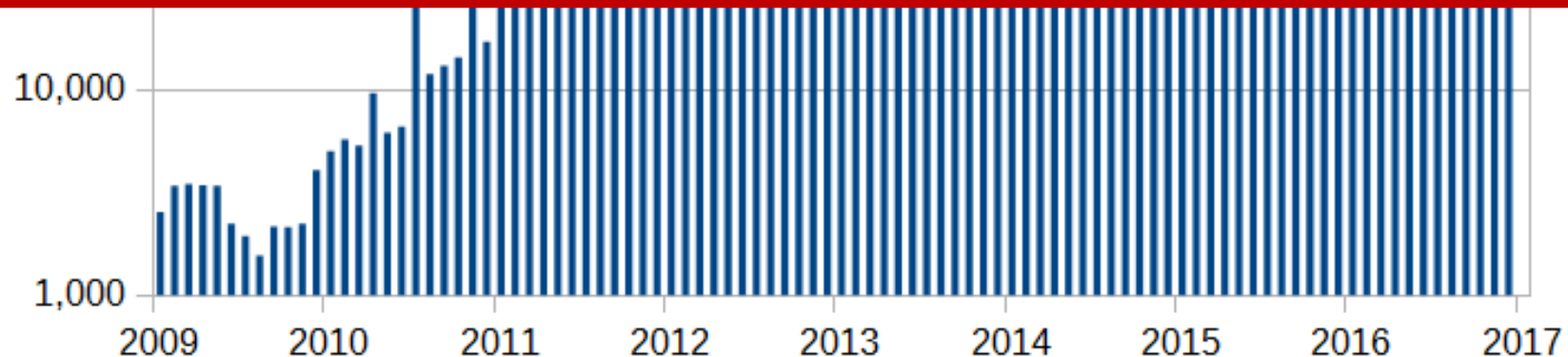
# Governance conflict

---

## The number of Bitcoin transaction per month

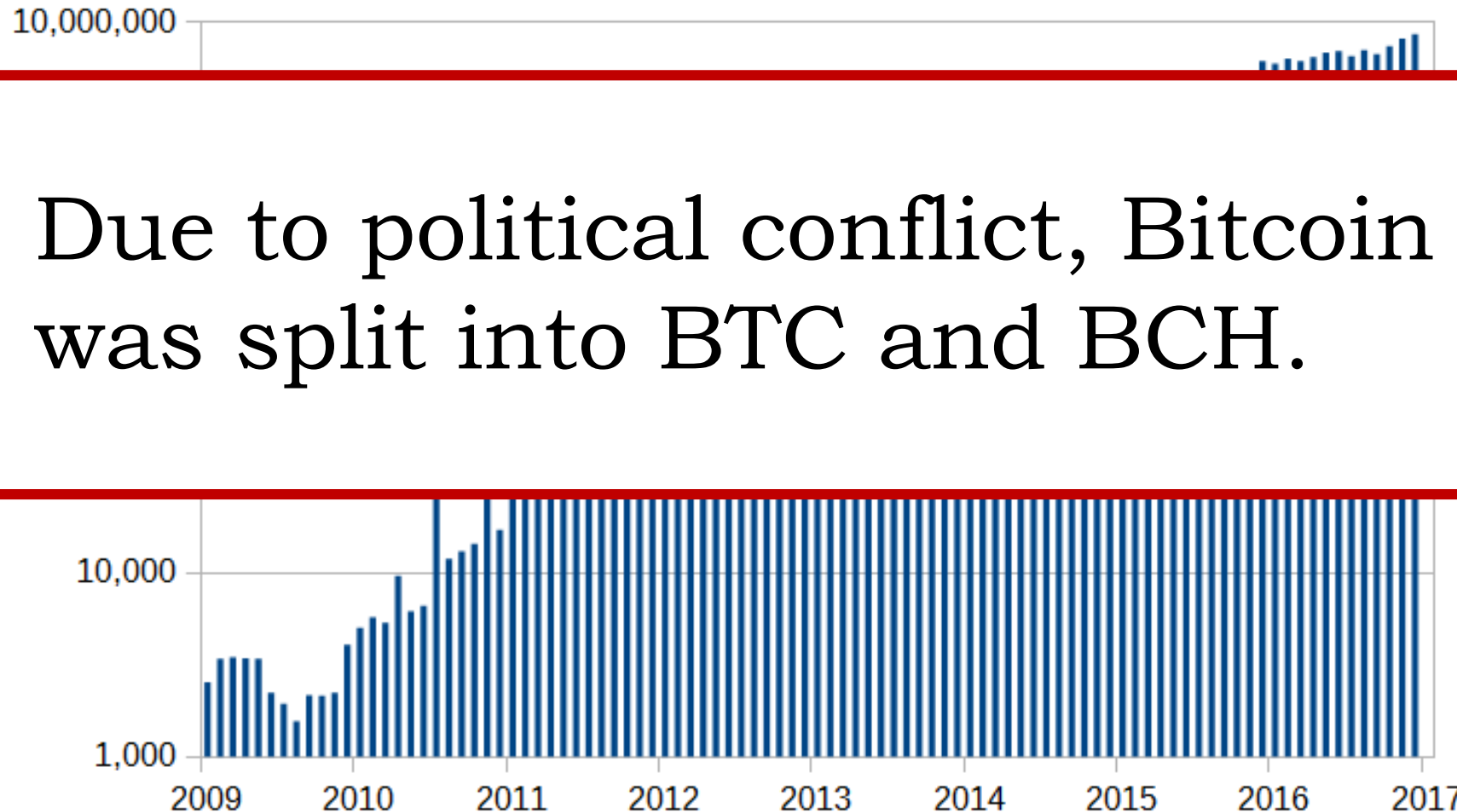


Several solutions were proposed.



# Governance conflict

## The number of Bitcoin transaction per month



# 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.



**Bitcoin (BTC)**

When it is more profitable to conduct **BTC mining**



**Bitcoin Cash (BCH)**

# Fickle mining

---

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



**Bitcoin (BTC)**

When it is more profitable to conduct **BCH** mining




**Bitcoin Cash (BCH)**




# Fickle mining

---

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

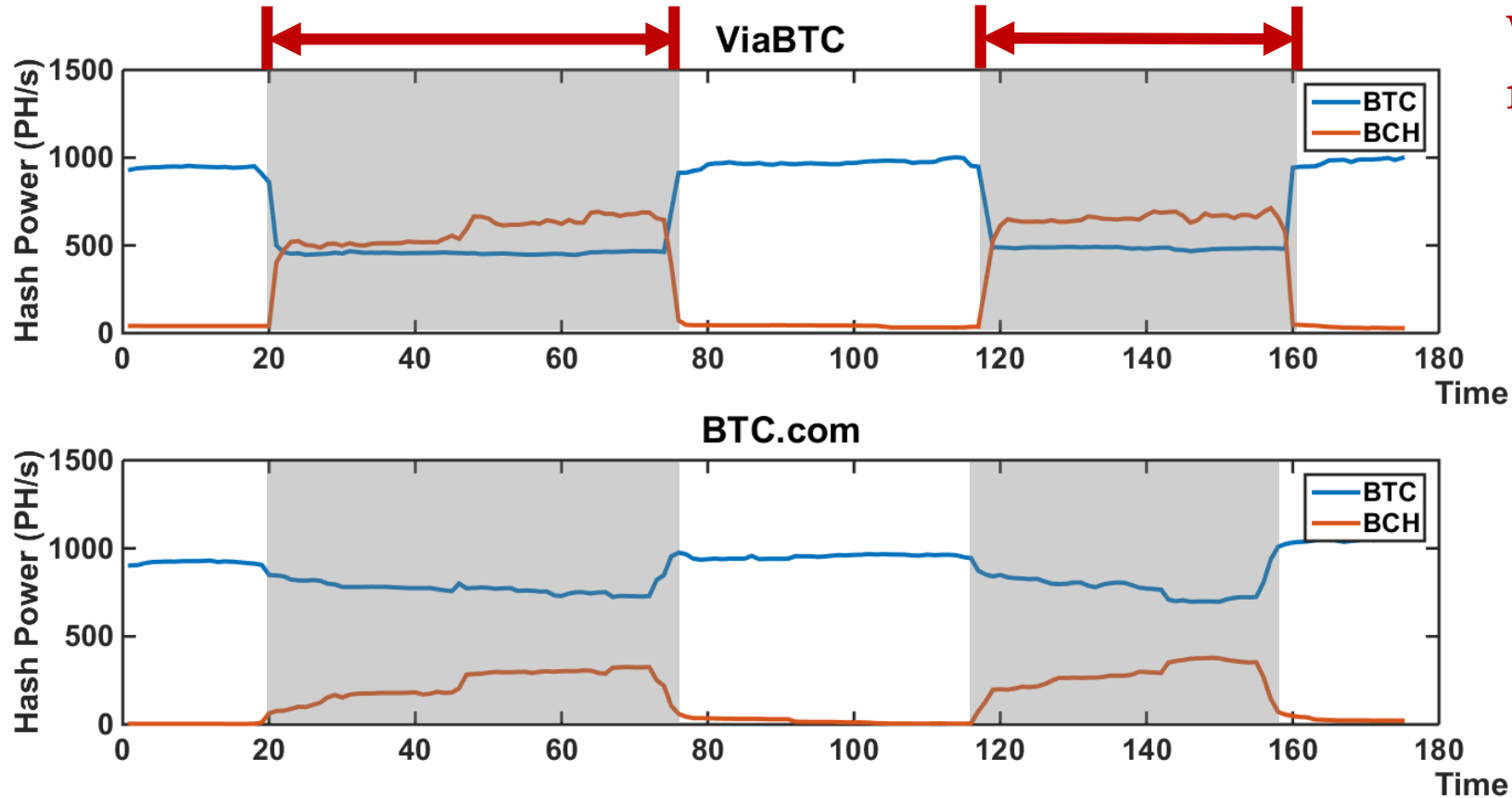


It is hard to predict the coin price.



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

# Fickle mining

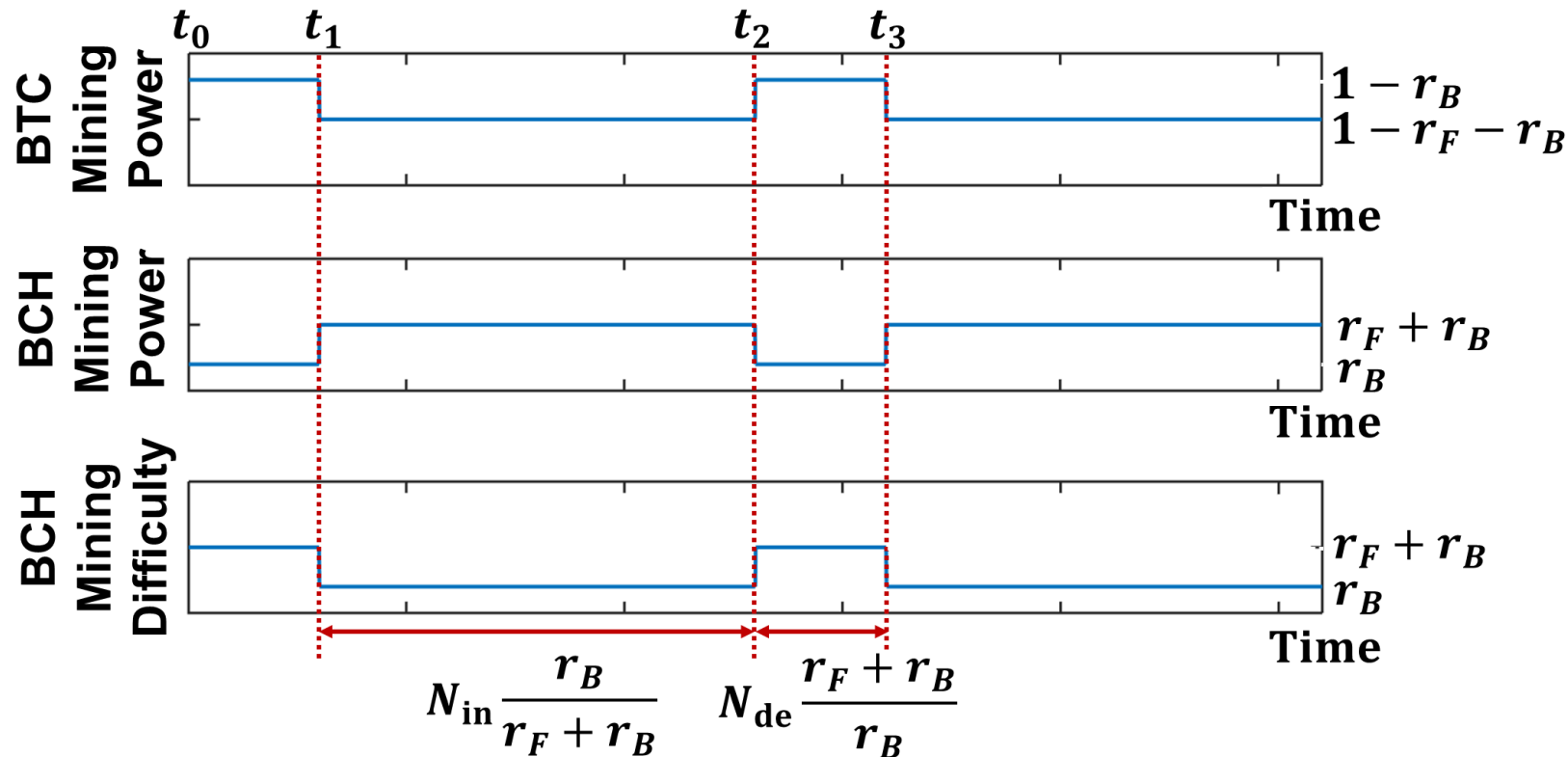


When BCH mining is easy

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

# Fickle mining

- ❖ The following 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.

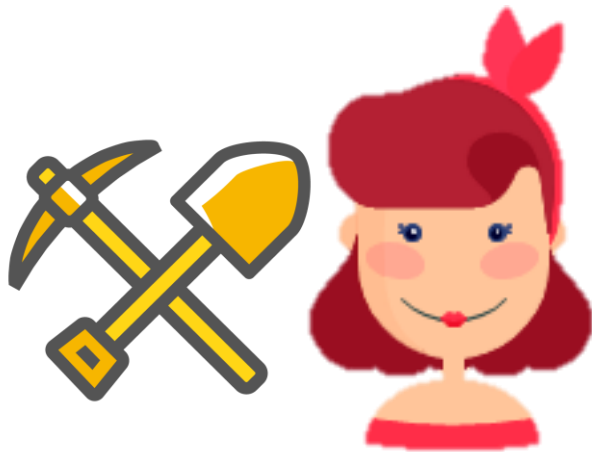


**Equilibrium in this situation?  
Change of mining power?**

# 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



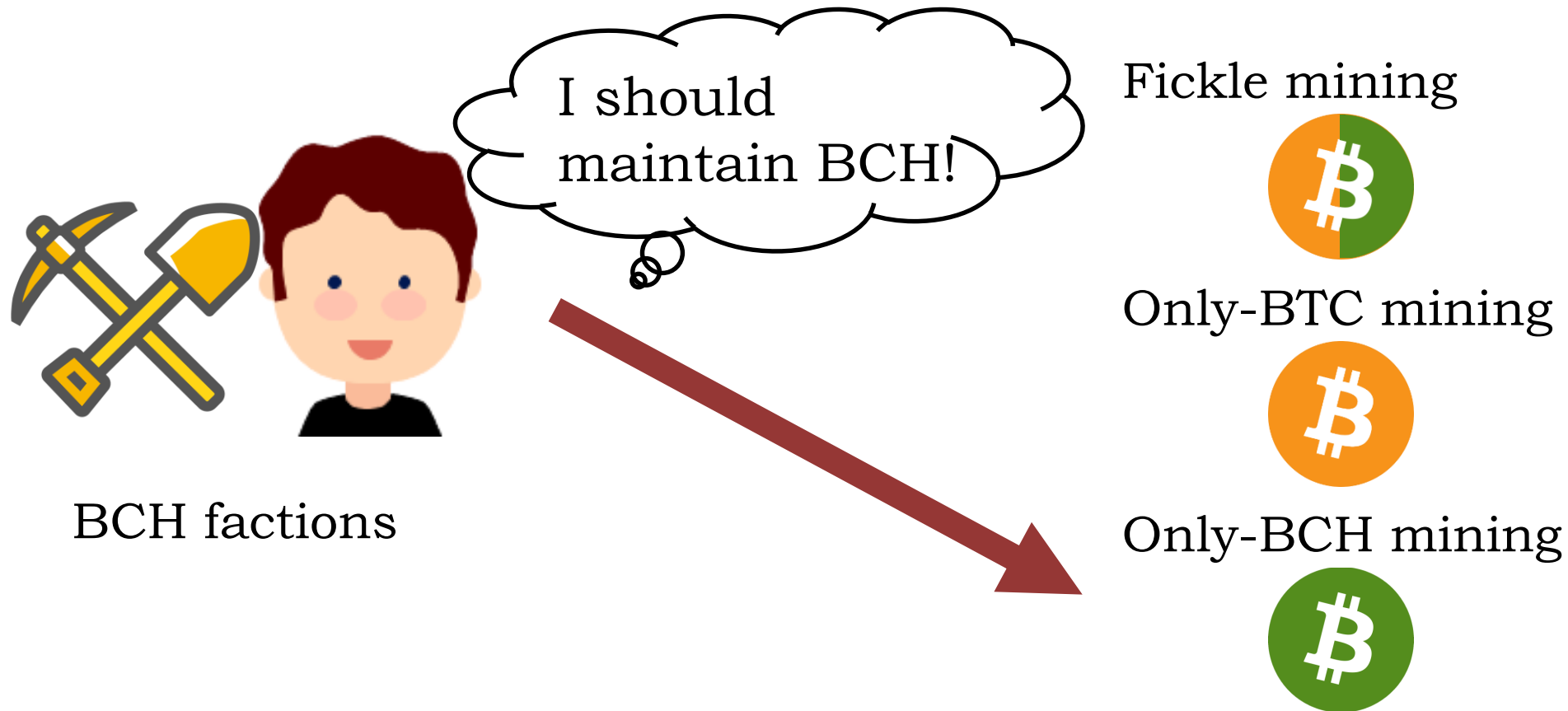
Only-BCH mining



# What is your choice?

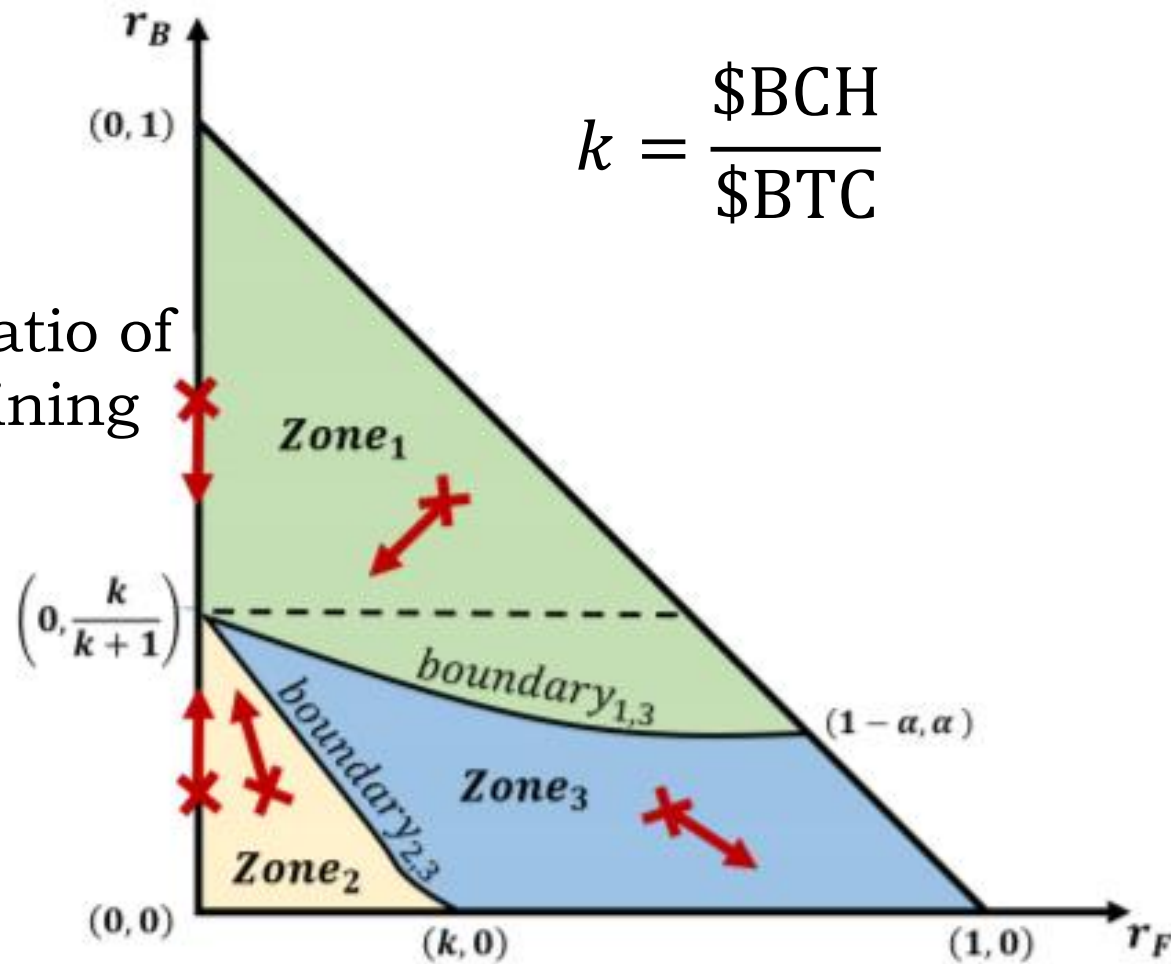
❖ Players: Many miners with small hash power

**Political BCH factions (e.g., BITMAIN)**



# Coexistence or downfall of BCH?

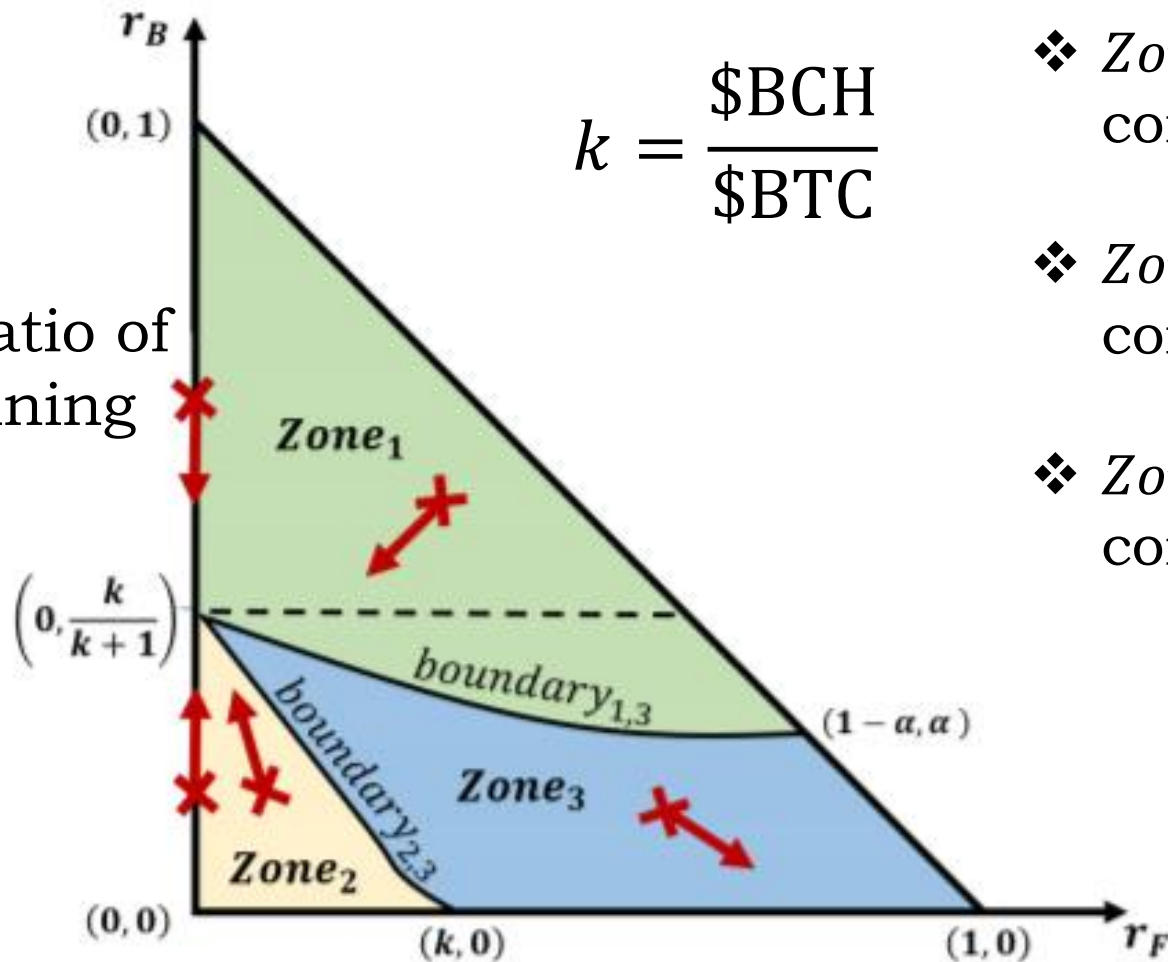
Hash power ratio of only-BCH mining



Hash power ratio of fickle mining

# Coexistence or downfall of BCH?

Hash power ratio of only-BCH mining



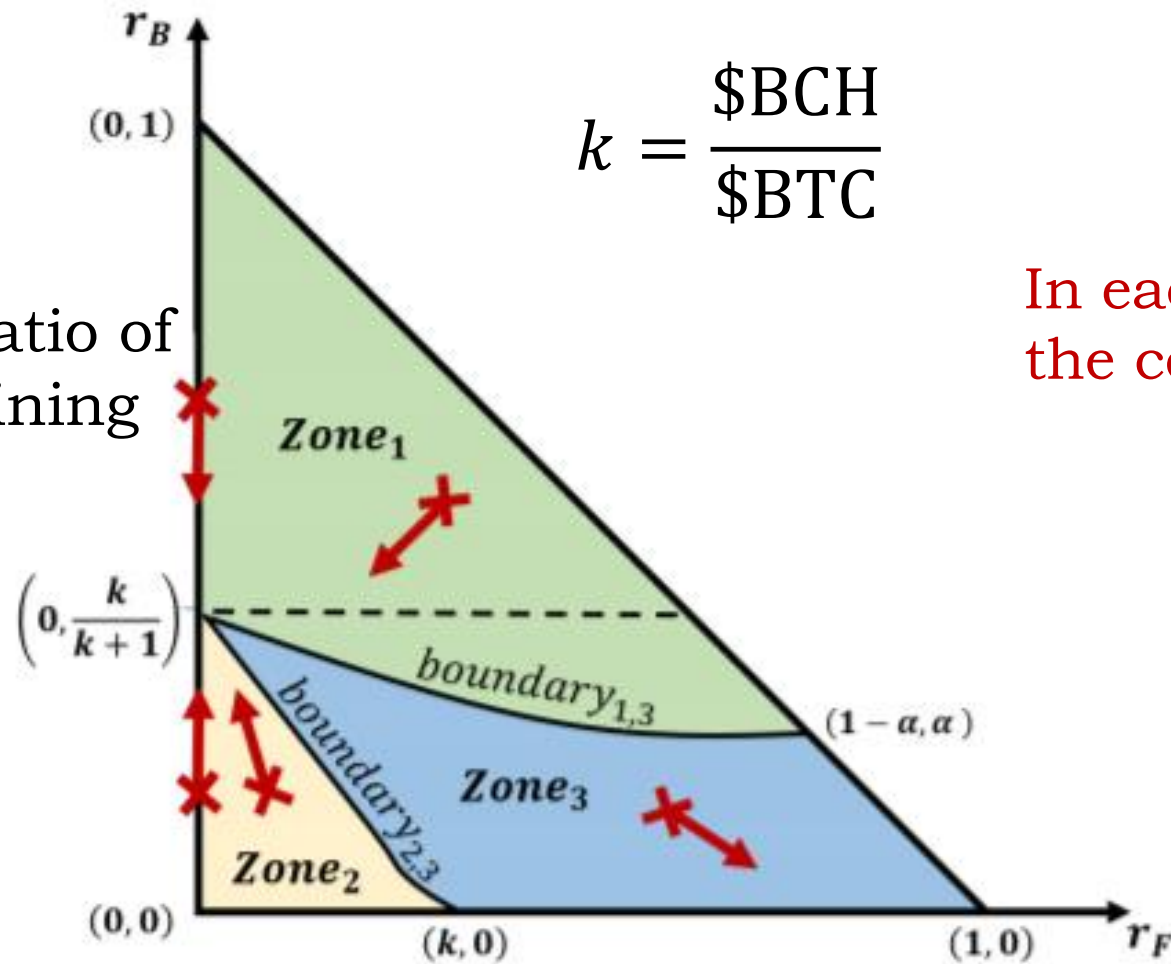
Hash power ratio of fickle mining

- ❖ Zone<sub>1</sub>: It is most profitable to conduct only-BTC mining.
- ❖ Zone<sub>2</sub>: It is most profitable to conduct only-BCH mining.
- ❖ Zone<sub>3</sub>: It is most profitable to conduct fickle mining.



# Coexistence or downfall of BCH?

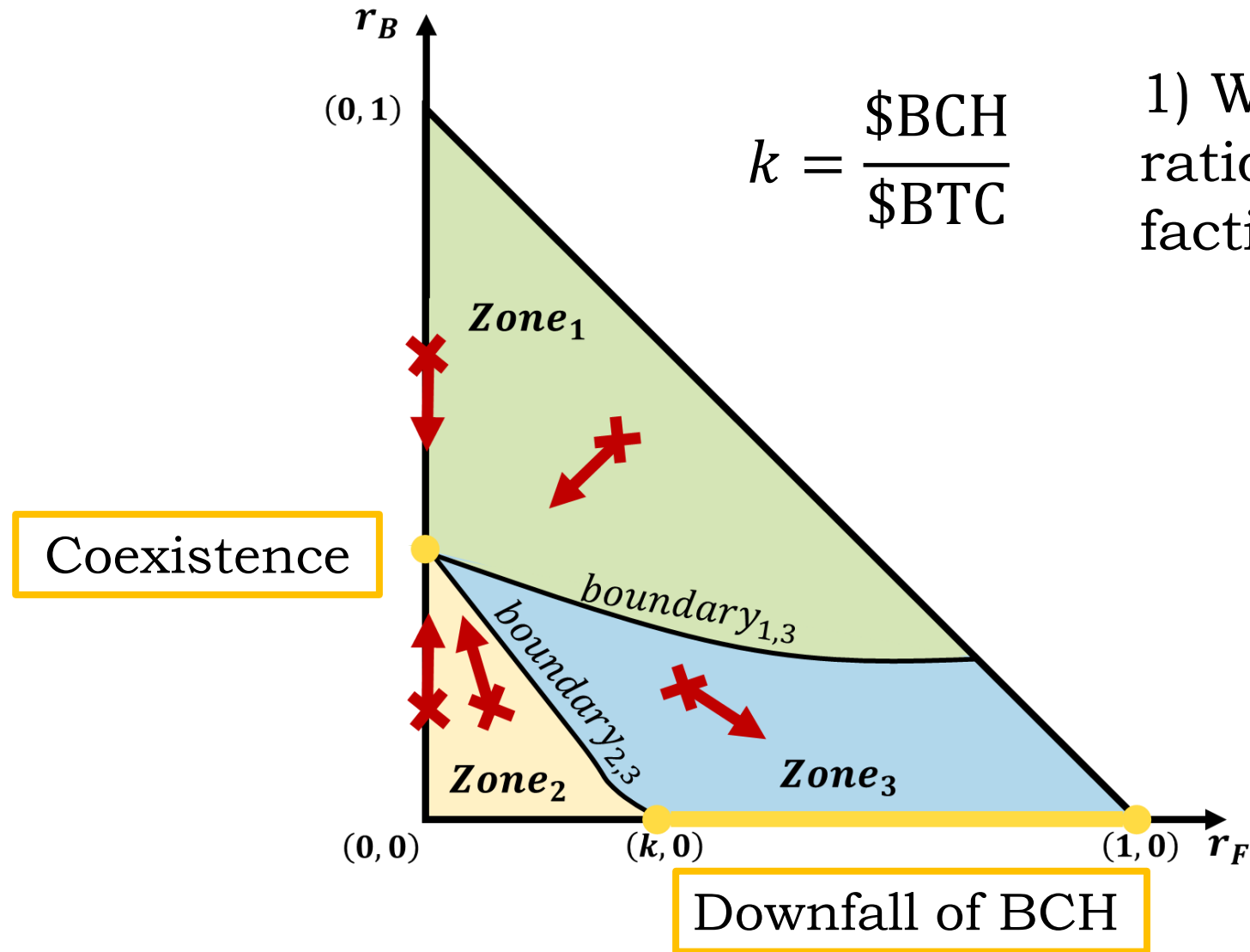
Hash power ratio of only-BCH mining



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

Hash power ratio of fickle mining

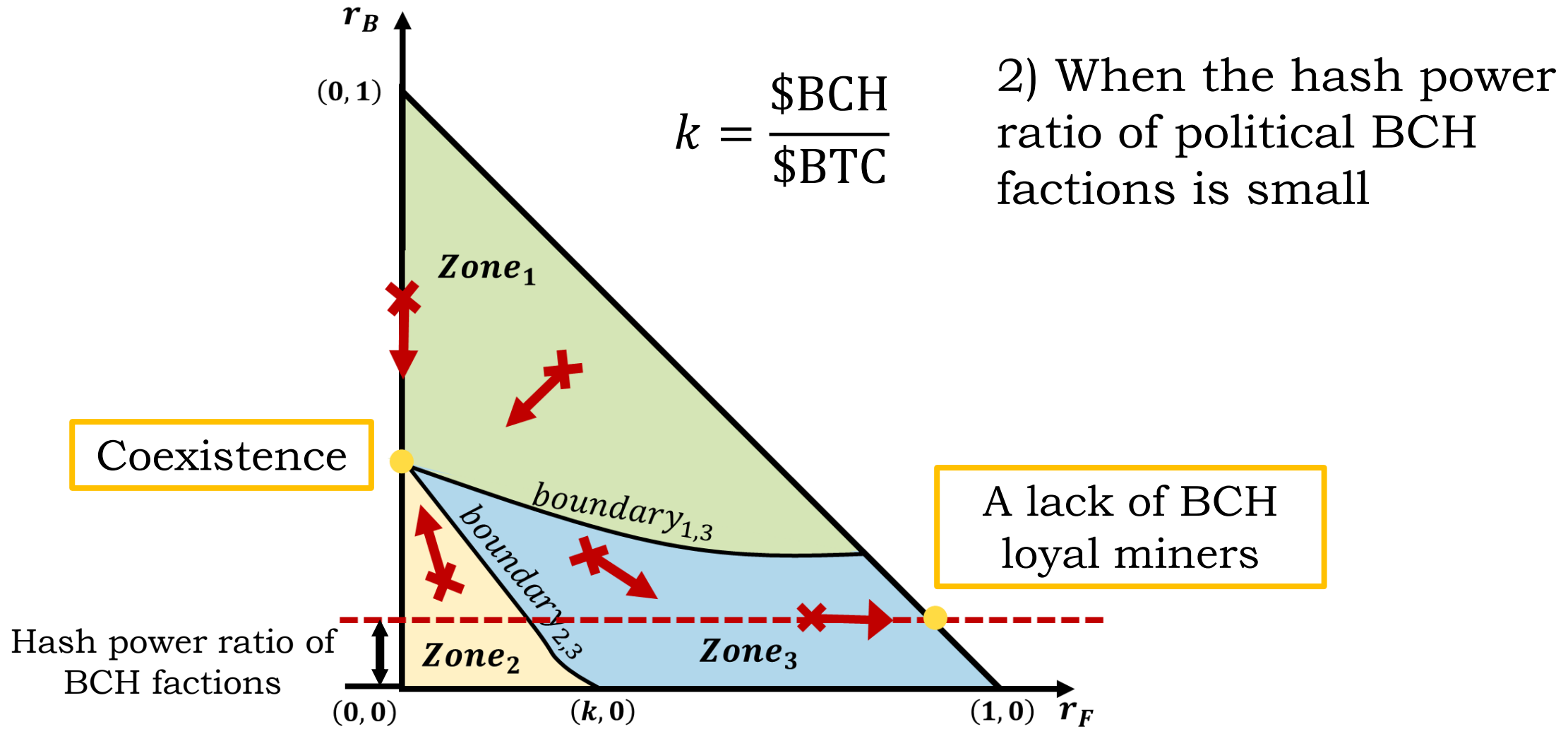
# Coexistence or downfall of BCH?



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

1) When the hash power ratio of political BCH factions is 0

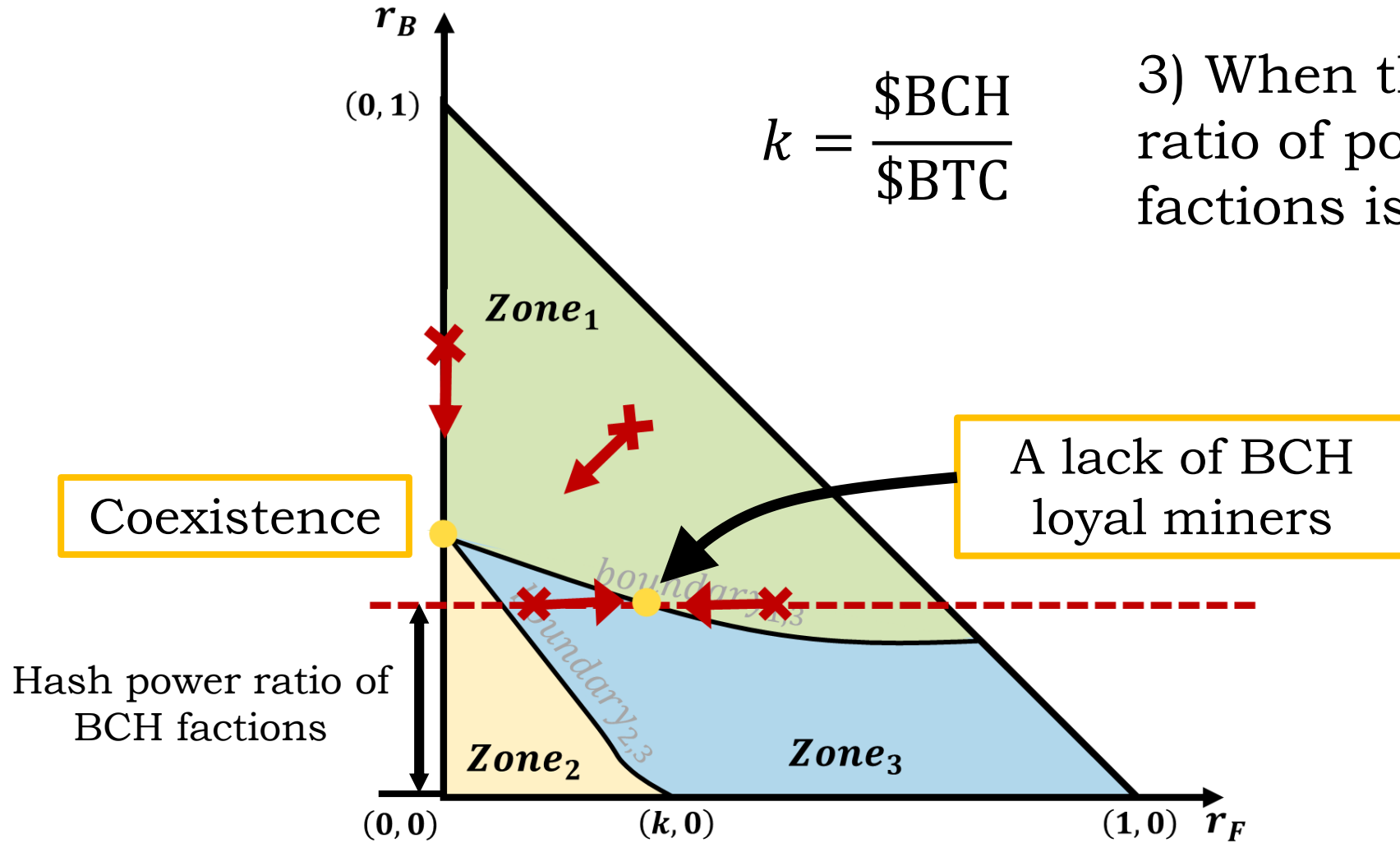
# Coexistence or downfall of BCH?



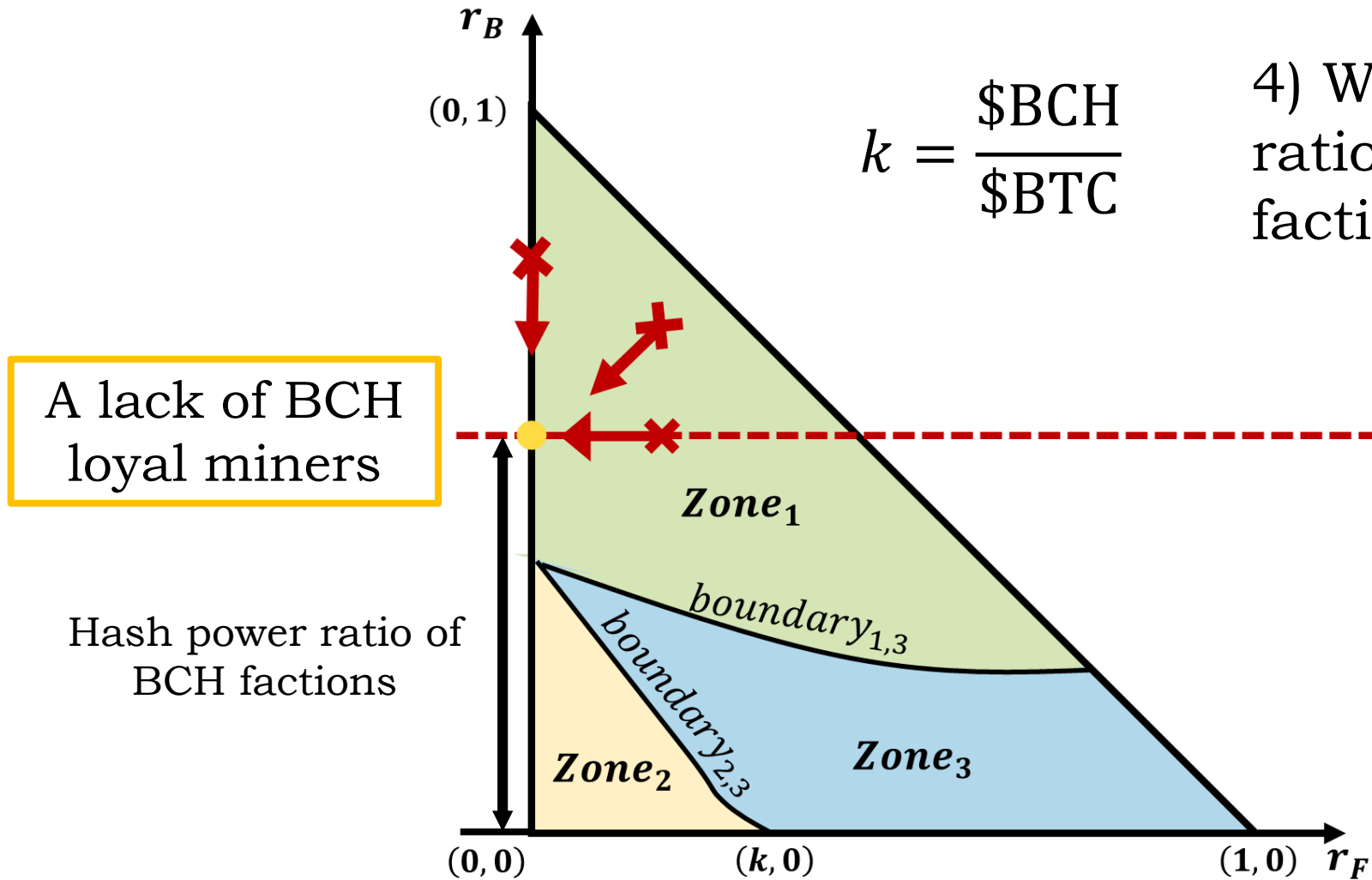
# Coexistence or downfall of BCH?

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

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



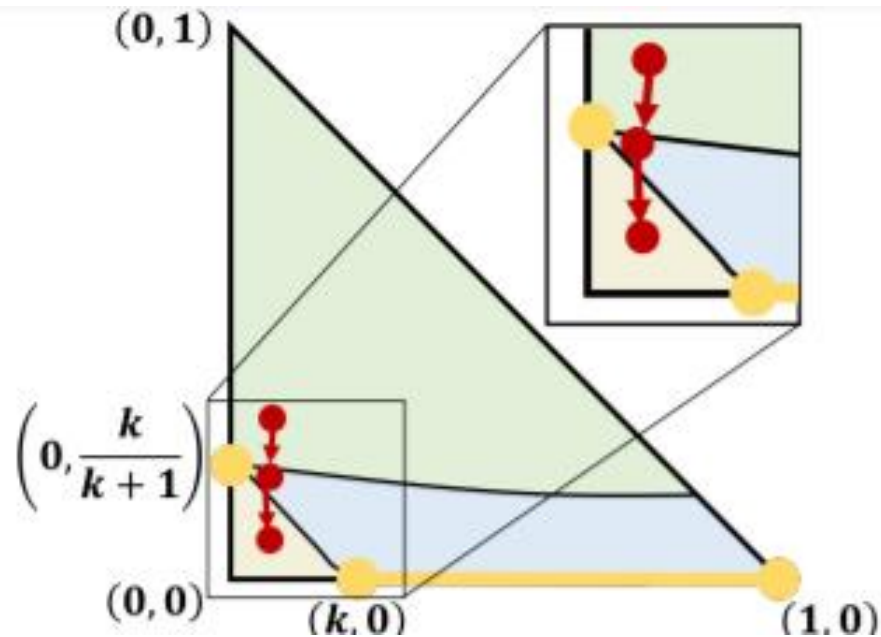
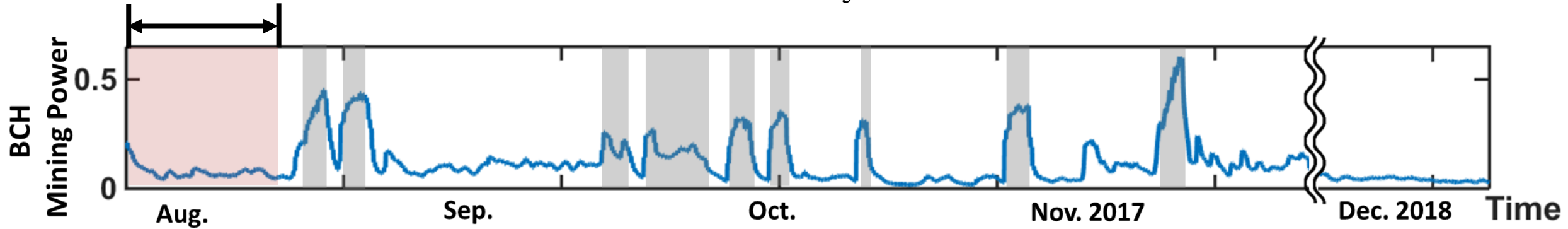
# Coexistence or downfall of BCH?



**What happened in practice?**

# 08/01/2017: Game start

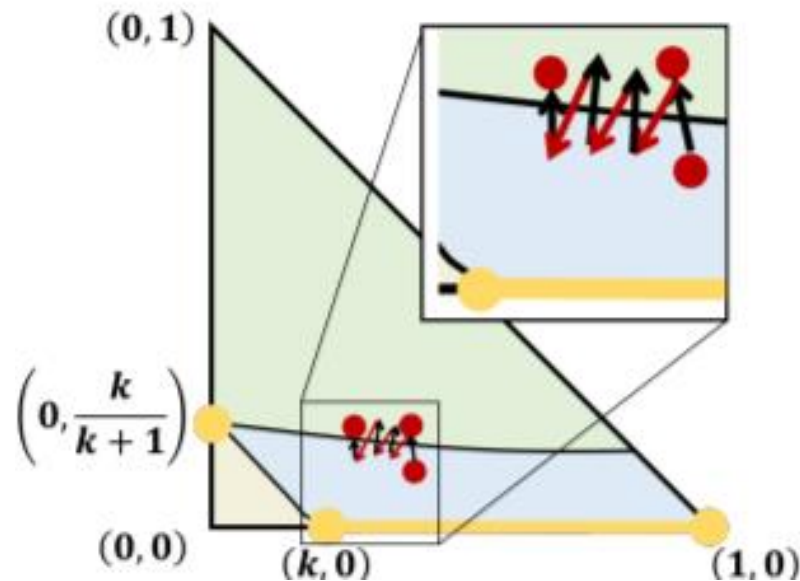
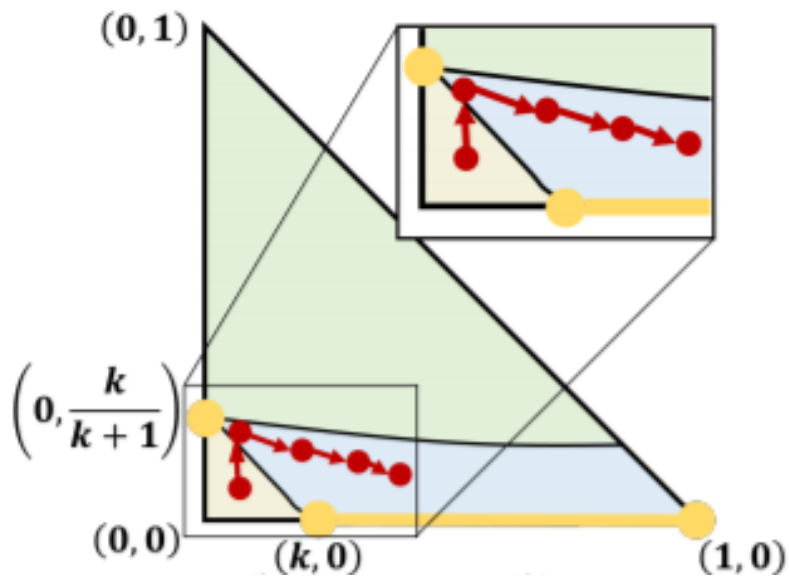
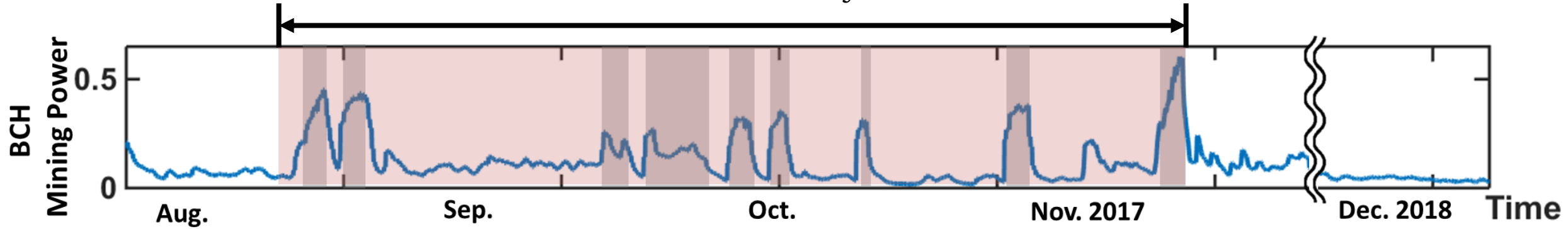
Hash rate history



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

# Before 11/13/2017

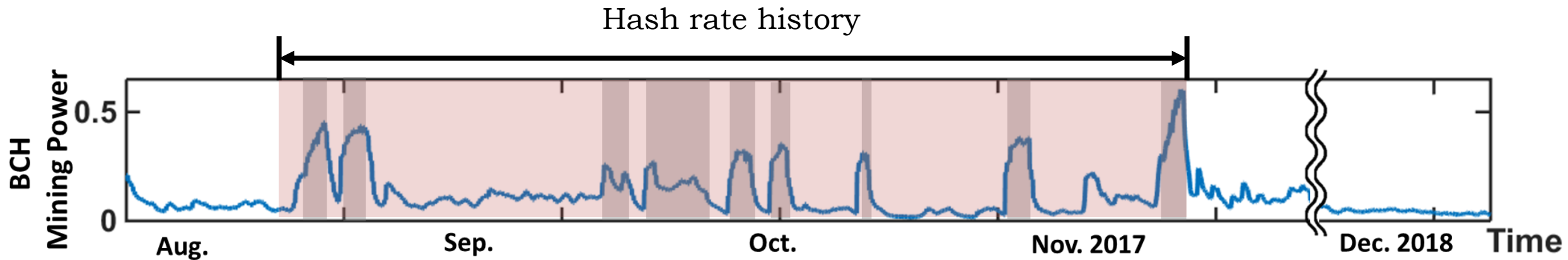
Hash rate history



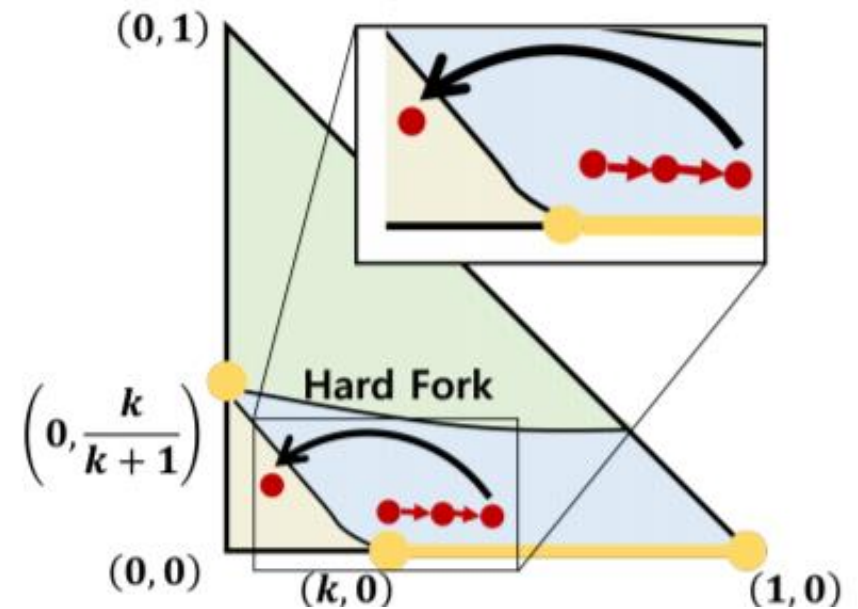
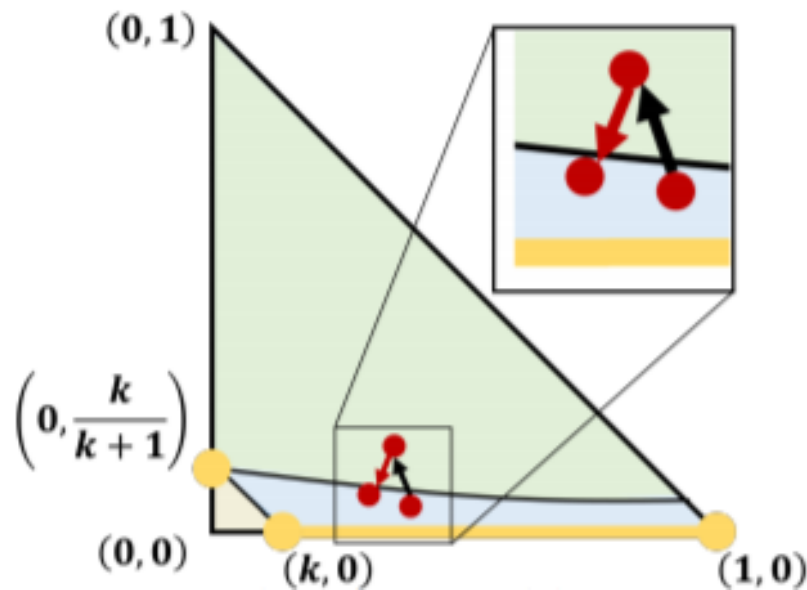
...



# Before 11/13/2017



...



# 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

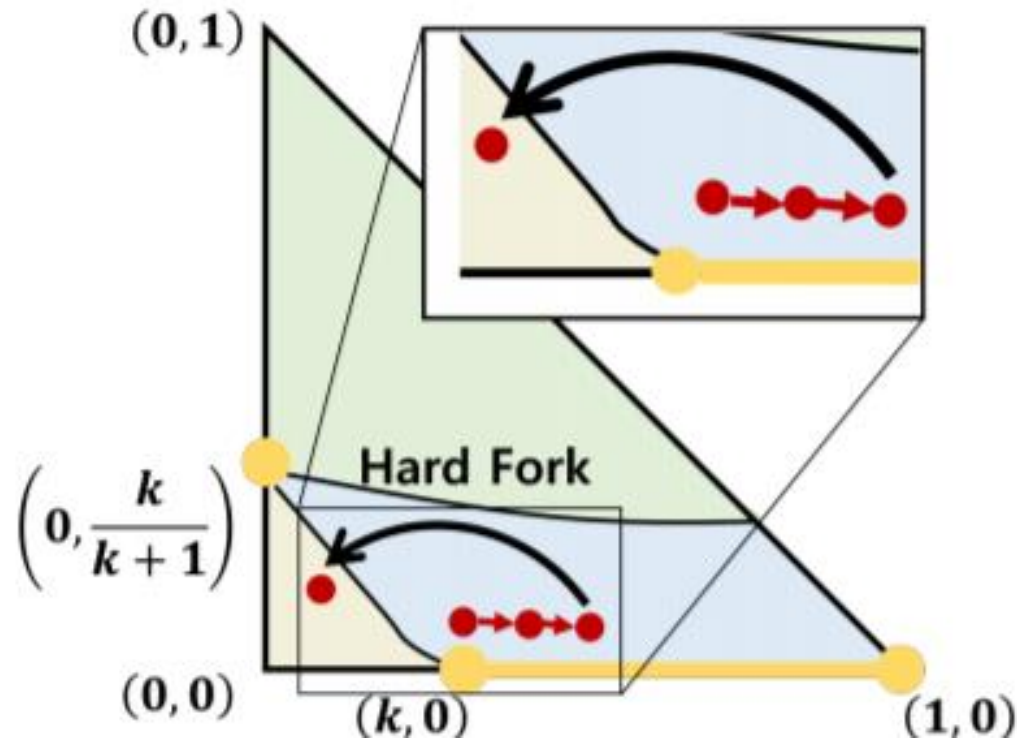
The Bitcoin ABC development team has announced its plans for the November 13 Hard Fork upgrade of Bitcoin Cash. The upgrade is designed to stabilize the problematic difficulty adjustment algorithm (DAA).

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

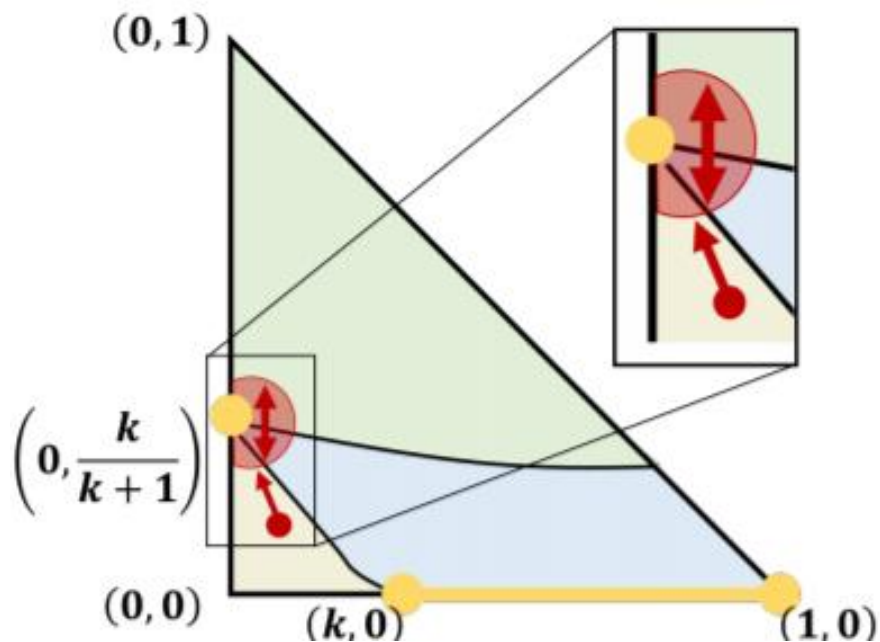
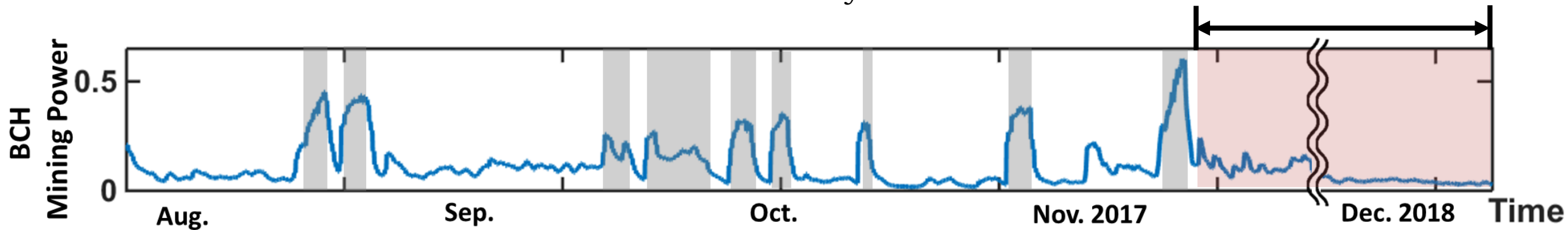
---



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

# After 11/13/2017

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.

The screenshot displays the Multipool website interface. At the top, the Multipool logo is on the left, and navigation links for Home, Pools, Stats, Help, Register, and Login are on the right. Below the navigation is a tabbed interface with 'Overview' selected. The main content area is divided into three columns, each representing a different mining algorithm: SHA-256, Scrypt, and X11. Each column features a 'Most Profitable' section with a coin icon, a list of coin options, and performance metrics. The SHA-256 section shows Bitcoin Cas as the most profitable, with metrics of 3.92 PH/s, 0.0418 /PH/s/d, and 110% BTC. The Scrypt section shows Litecoin as the most profitable, with metrics of 61.47 GH/s and 0.0005 /GH/s/d. The X11 section shows Dash as the most profitable, with metrics of 2.91 TH/s and 0.0092 /TH/s/d. Below the main content, there is a 'Welcome to Multipool!' message, a 'Recent News' section with two news items, a warning about phishing and scams, and a 'Recent Profitability' section with a link to 'Average Profitability'.

**MULTIPOOL** Home Pools Stats Help Register Login

Overview SHA-256 Scrypt X11

**SHA-256 Most Profitable**

 Bitcoin Cas


NMC

SYS

XMY

3.92 PH/s 0.0418 /PH/s/d 110% BTC

**Scrypt Most Profitable**


 Litecoin

DOGE

VIA

61.47 GH/s 0.0005 /GH/s/d

**X11 Most Profitable**

 Dash

UIS

2.91 TH/s 0.0092 /TH/s/d

Welcome to Multipool!

**Recent News**

**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 Moza (\$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](mailto:admin@multipool.us).

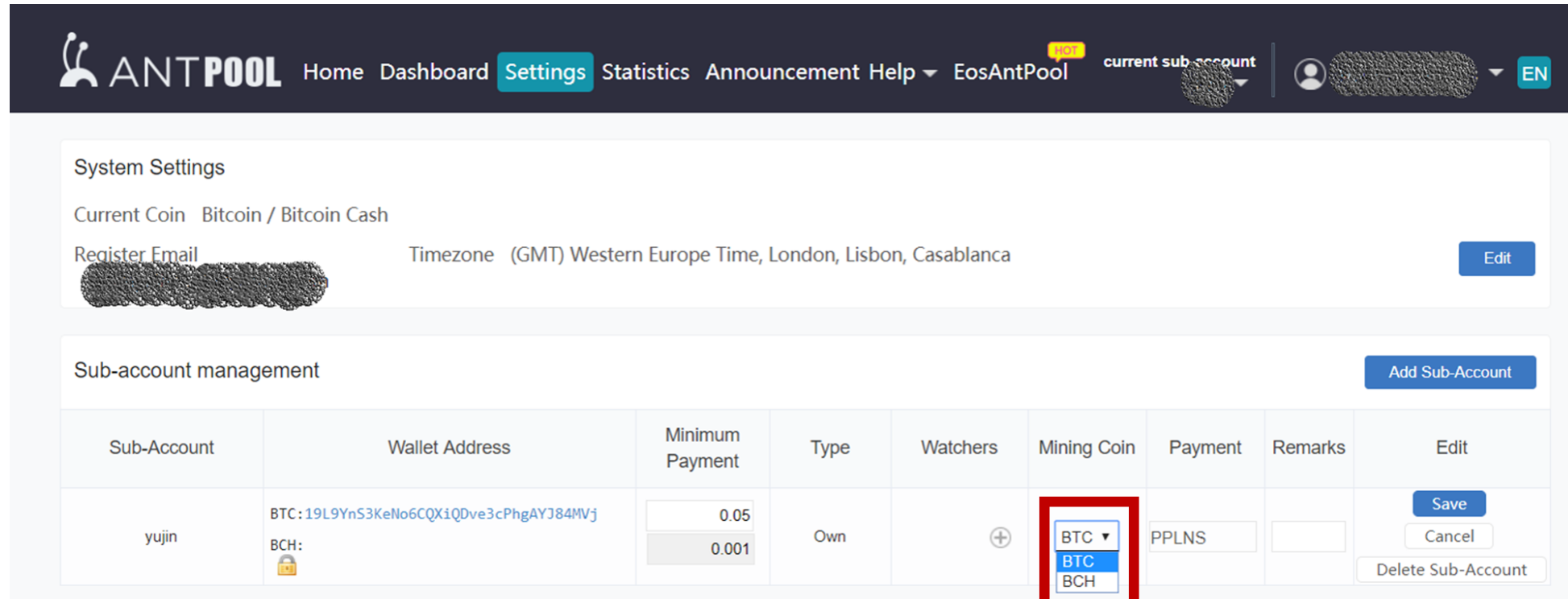
**Recent Profitability**

Average Profitability



# Automatic mining

- ❖ Miners can automatically choose the most profitable coin.



The screenshot shows the ANTPool web interface. The top navigation bar includes 'ANTPOOL', 'Home', 'Dashboard', 'Settings', 'Statistics', 'Announcement', and 'Help'. The 'Settings' tab is active. Below the navigation bar, the 'System Settings' section shows 'Current Coin' set to 'Bitcoin / Bitcoin Cash' and 'Timezone' set to '(GMT) Western Europe Time, London, Lisbon, Casablanca'. The 'Sub-account management' section features a table with columns: Sub-Account, Wallet Address, Minimum Payment, Type, Watchers, Mining Coin, Payment, Remarks, and Edit. A sub-account named 'yujin' is listed with a Bitcoin address and a minimum payment of 0.05. A dropdown menu for 'Mining Coin' is highlighted with a red box, showing options for 'BTC' and 'BCH'. A red arrow points from this dropdown to the text 'One-button switch' below.

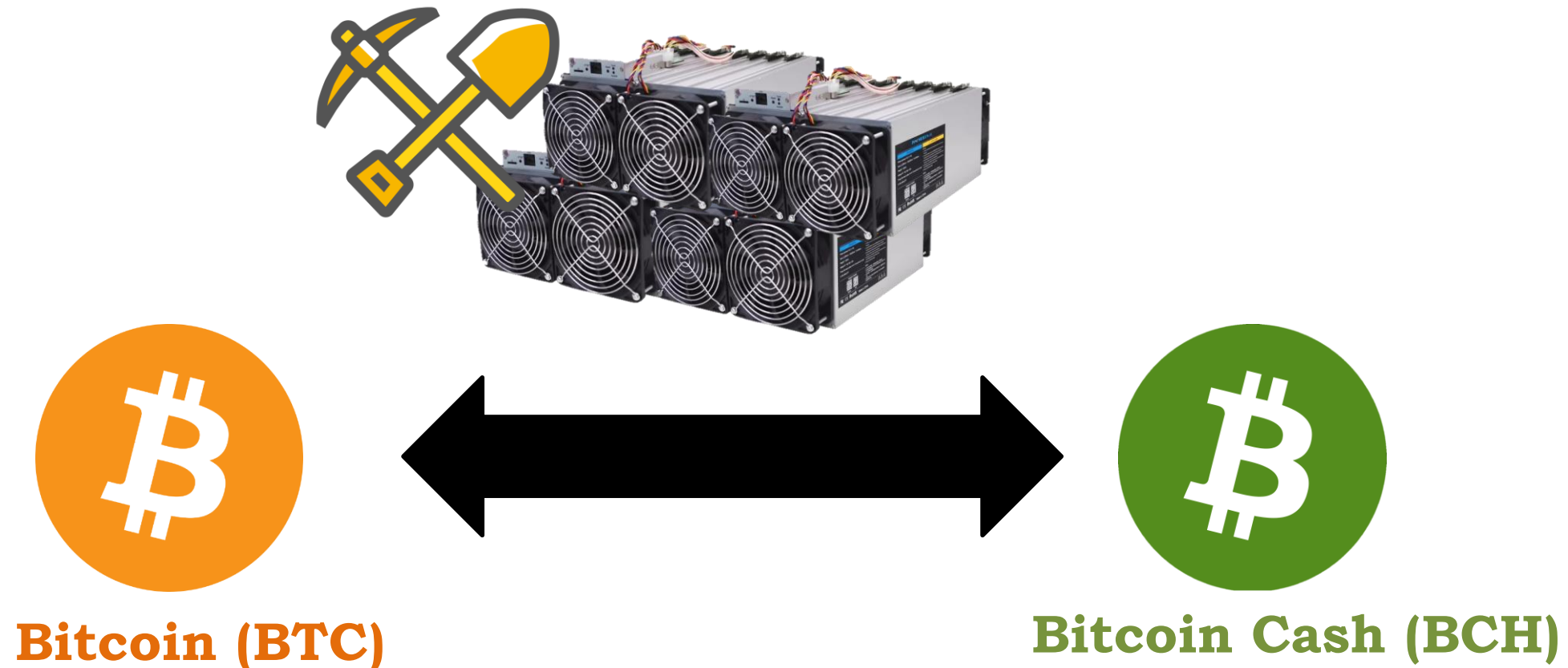
Sub-Account	Wallet Address	Minimum Payment	Type	Watchers	Mining Coin	Payment	Remarks	Edit
yujin	BTC: 19L9YnS3KeNo6CQX1QDve3cPhgAYJ84MVj BCH:	0.05 0.001	Own		BTC BCH	PPLNS		Save Cancel Delete Sub-Account

**One-button switch**

# Automatic mining

---

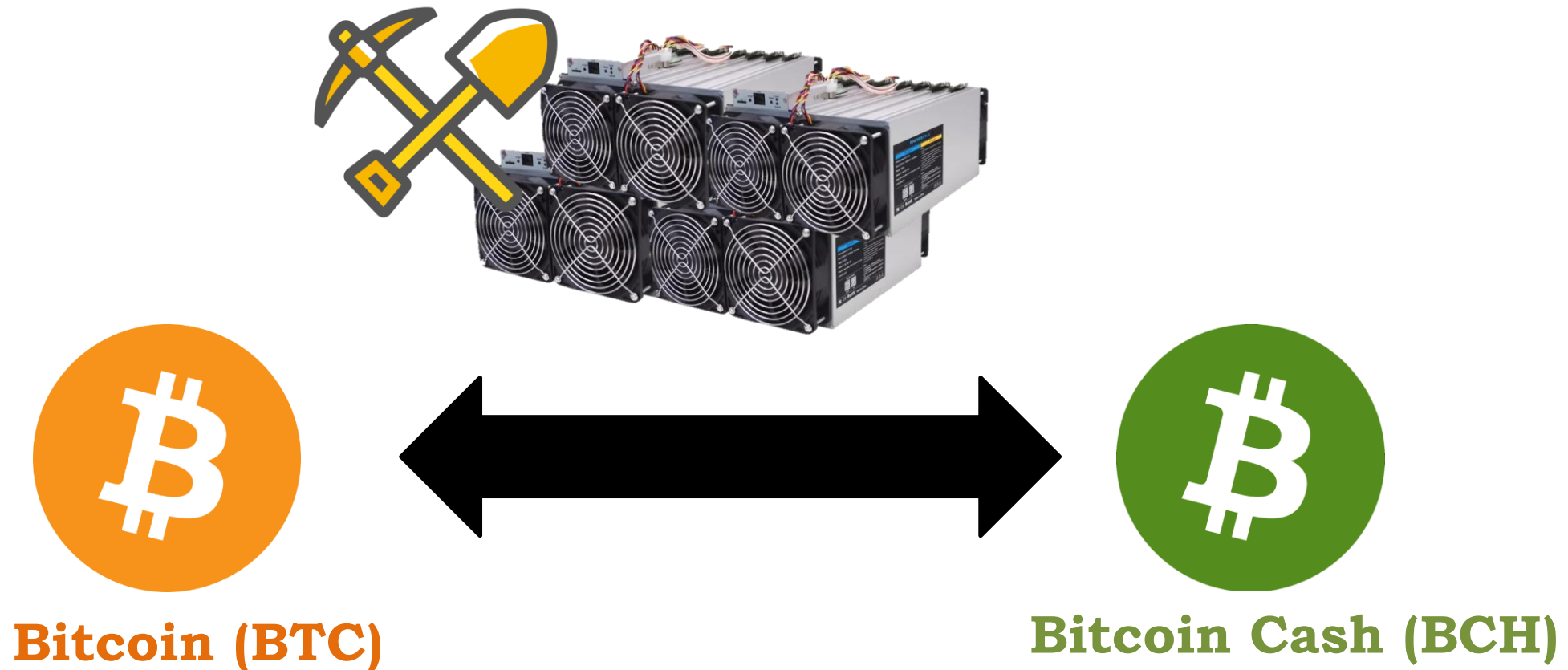
- ❖ When **the coin price or mining difficulty** changes, miners can immediately switch the coin to be mined.



# Fickle mining

---

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



# Automatic mining

---

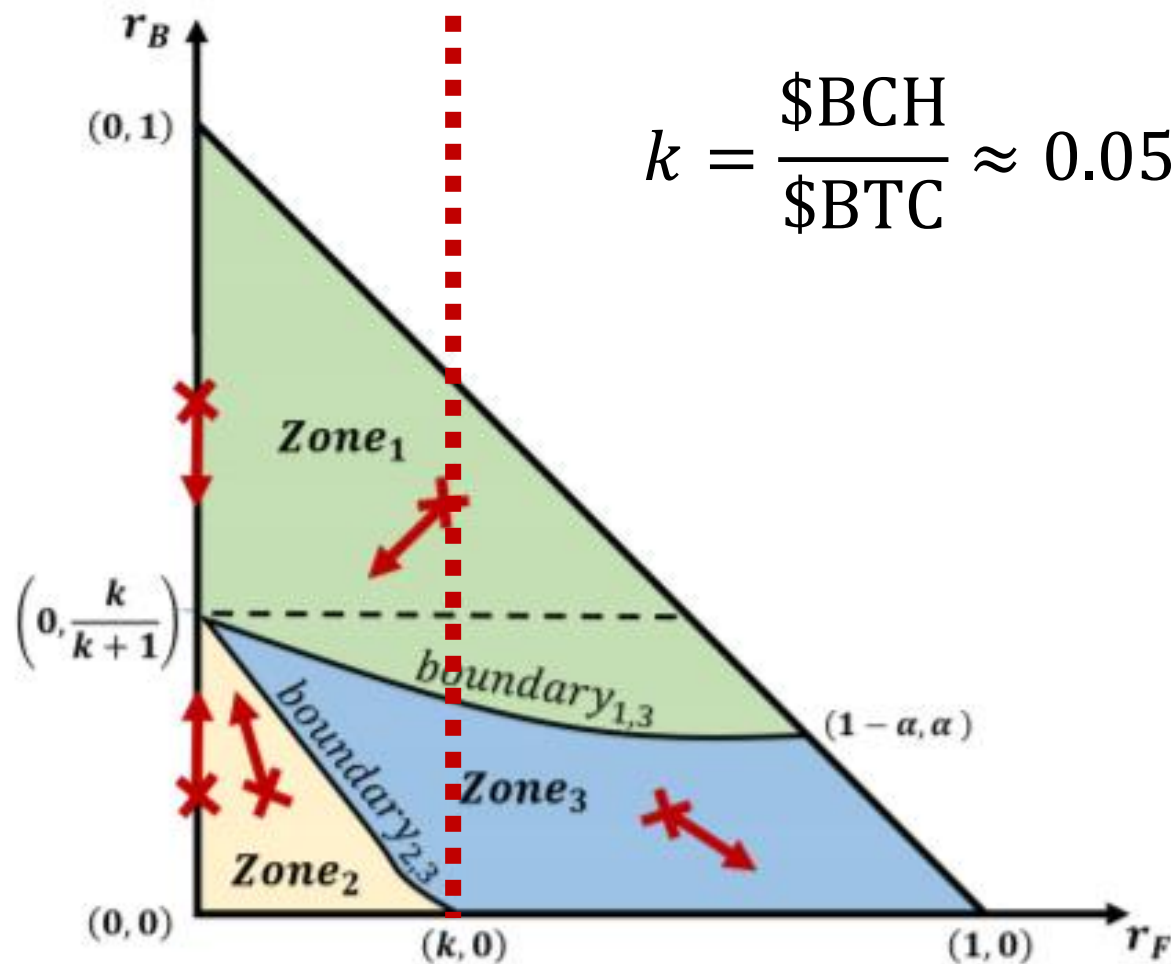
- ❖ When **the coin price or mining difficulty** changes, miners

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*.

**Bitcoin (BTC)**

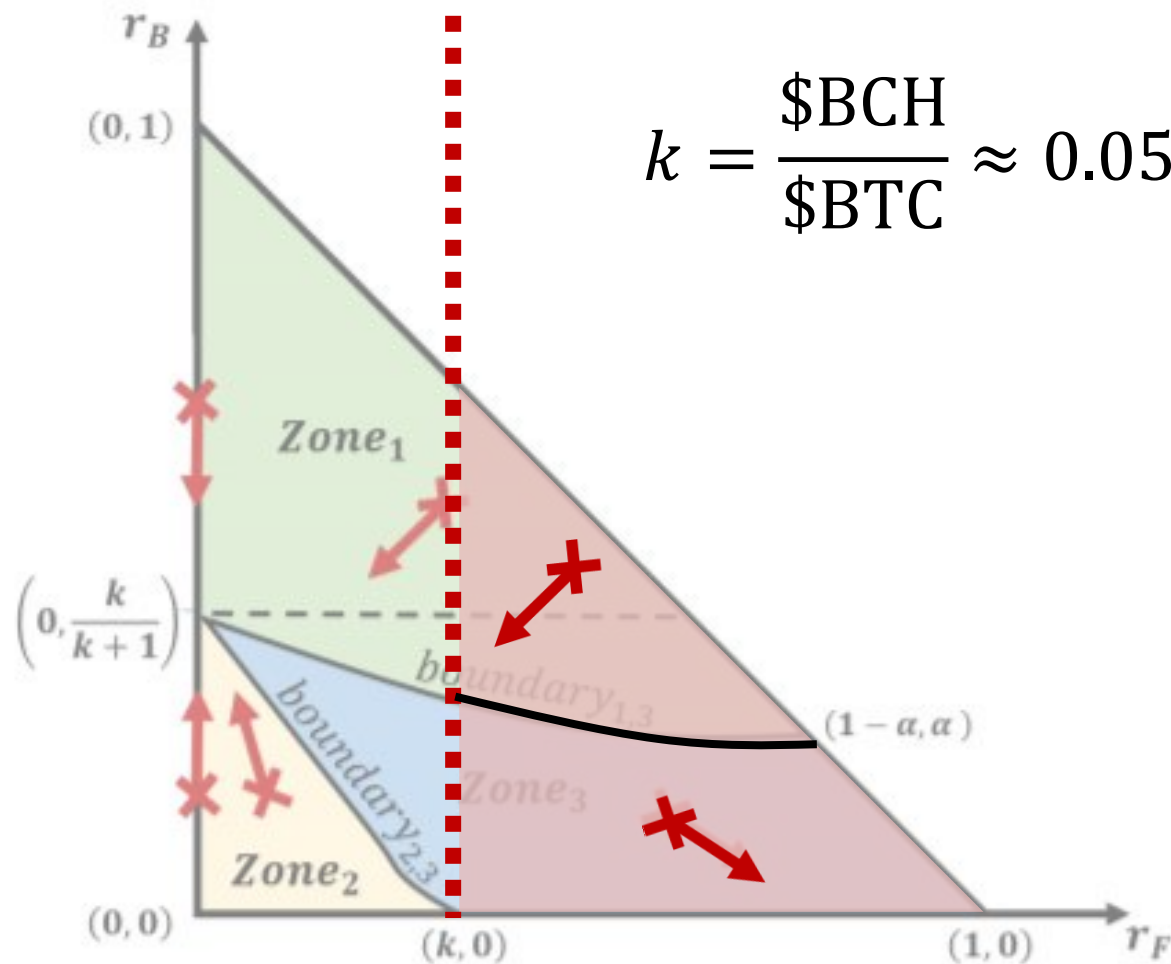
**Bitcoin Cash (BCH)**

# Automatic mining



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.

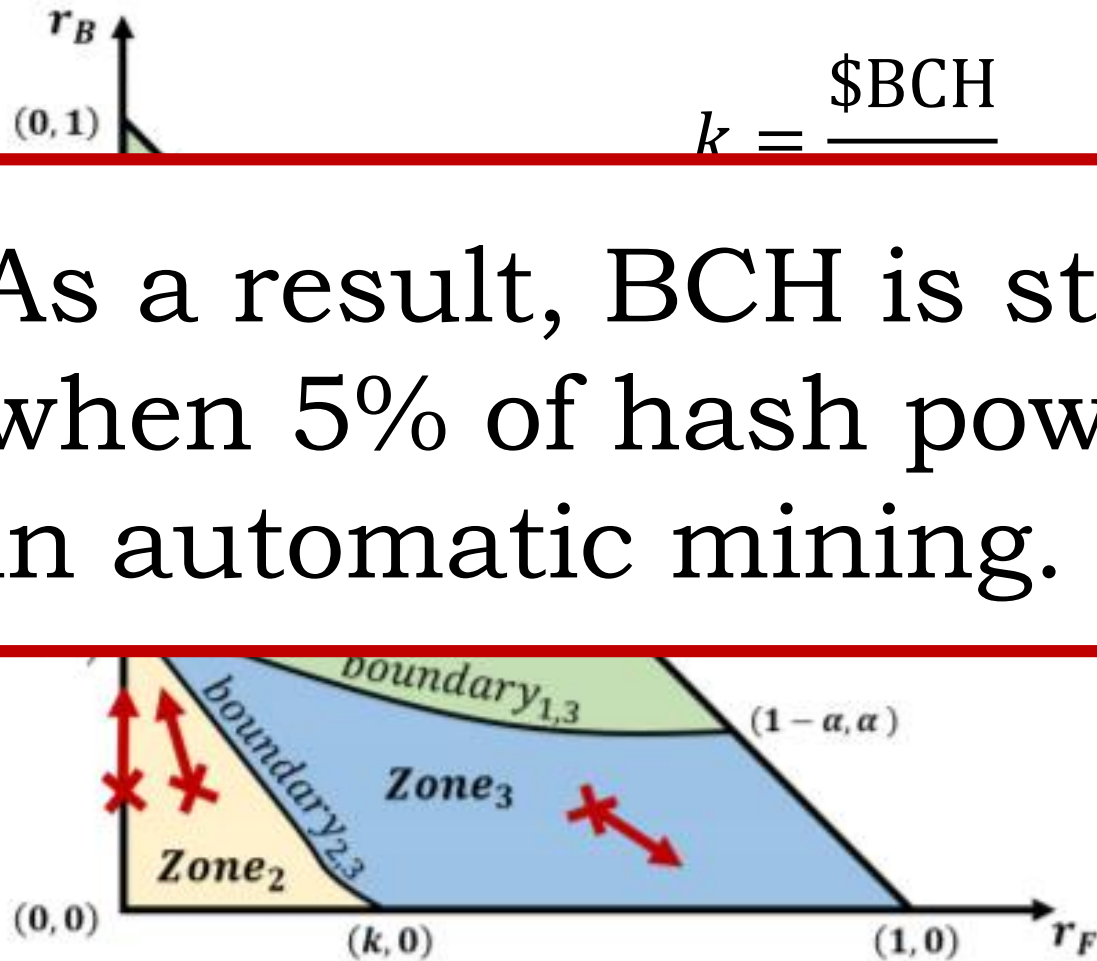
# Automatic mining



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.



# Automatic mining



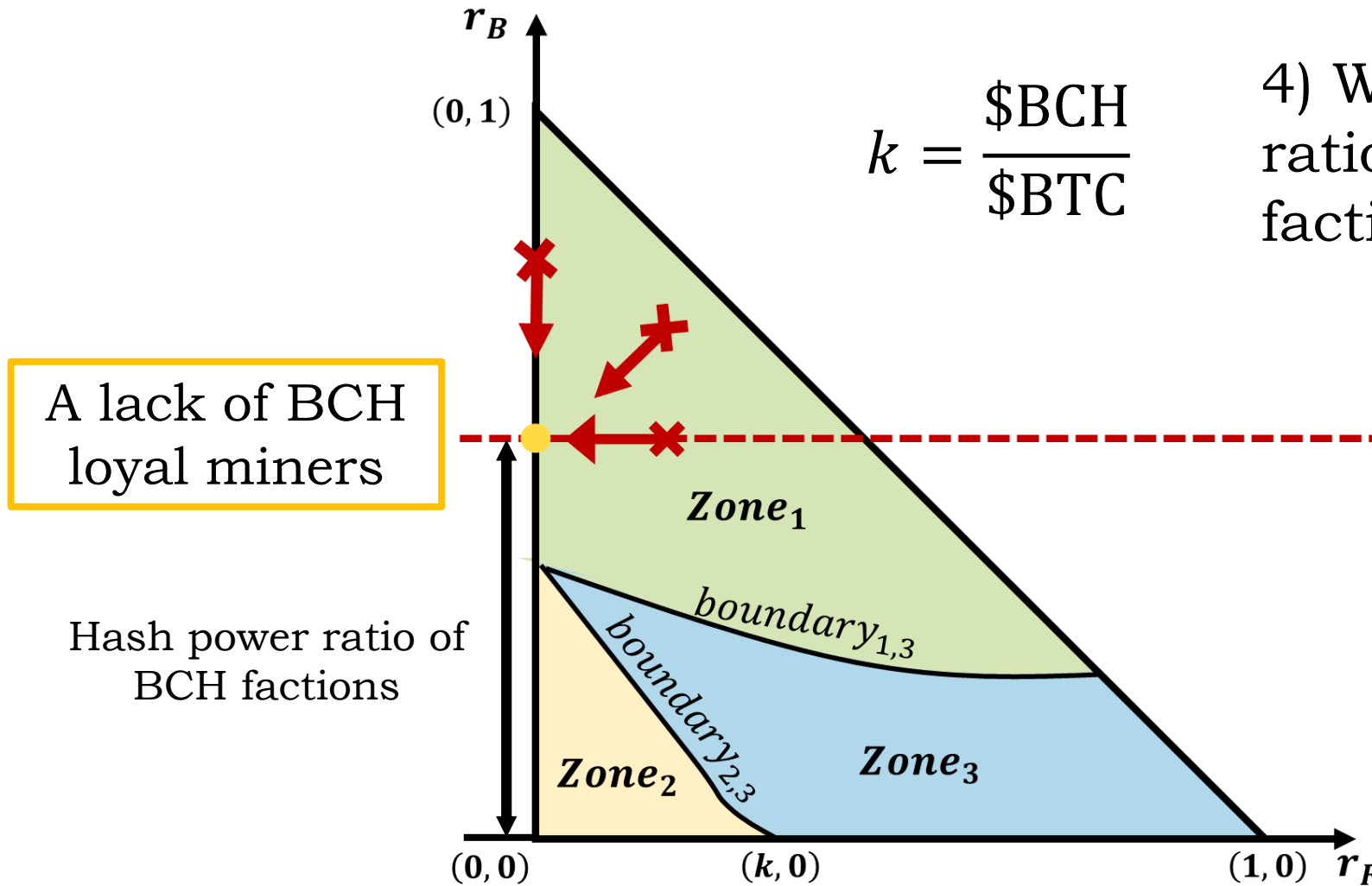
As a result, BCH is still not safe, when 5% of hash power is involved in automatic mining.

of BCH-loyal miners.

# **Bitcoin ABC vs. Bitcoin SV: Hash war**



# Coexistence or downfall of BCH?



# **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!**