Bitcoin Cash Split

What Happened?

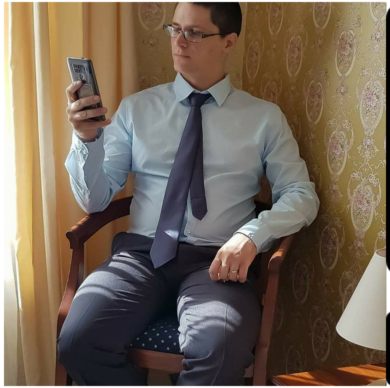
by Aleksandar Dinkov (@BitcoinSofia)

Who am I ?

- A Programmer, or...
  Large Scale Test Automation Software Developer
  (I test scalability)

- A man who knows a few Economic Terms
  (aka “Has a diploma from an Economy University - UNWE”)

- Organizer of “Bitcoin Cash Sofia Meetup”?



Scan me

alexander.n.dinkov@gmail.com
+359883332088
https://github.com/Siko91
https://www.facebook.com/siko1991

http://bitcoinsofia.com
http://pipe.cash
http://bitcoinfizzbuzz.com

Who am I ?

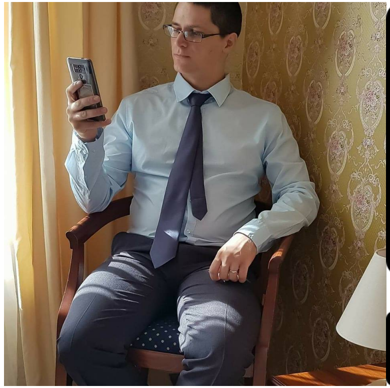
- A Programmer, or...
  Large Scale Test Automation Software Developer
  (I test scalability)

- A man who knows a few Economic Terms
  (aka “Has a diploma from an Economy University - UNWE”)

- Organizer of “Bitcoin Cash Sofia Meetup”?

- A person who can kick ass
  (I do martial arts)

Please be civilized with your questions...



Scan me

alexander.n.dinkov@gmail.com
+359883332088
https://github.com/Siko91
https://www.facebook.com/siko1991

http://bitcoinsofia.com
http://pipe.cash
http://bitcoinfizzbuzz.com

Plan

Facts	**Opinions**
- Who is Who	- <see facts>
- What code changes were made	- <see facts>
- <see opinions>	- Drama and Threats
- <see opinions>	- Misconceptions
- Which is the Real Bitcoin Cash	- <see facts>
- Hash War	- <see facts>
- <see opinions>	- Tribalism
- <see opinions>	- My Choice

Who is Who

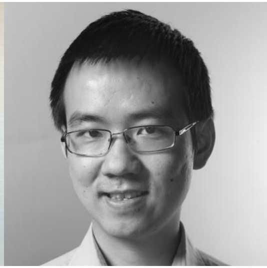
Craig Wright

Calvin Aire

Steve Shadders

Ryan X. Charles

Roger Ver



Jihan Wu

Amaury Séchet

Peter Ruzin

Code Changes

Bitcoin SV	Bitcoin Cash
- Scripts Length Limit : 201 to 500 - Default Block Size : 32 MB to 128 MB - Unlocked Scripts : OP_MUL, OP_INVERT, OP_LSHIFT, & OP_RSHIFT	- Replace topological ordering constraint with canonical transaction order - New Script Codes : OP_CHECKDATASIG and OP_CHECKDATASIGVERIFY
All of these changes are also in the Bitcoin Cash Roadmap. They were supposed to happen during May 2019.	These changes were rejected by the Bitcoin SV side. The disagreement about these changes is what caused the split.
These changes are basically just removals of limitations. The code is the same, but it simply operates more freely.	These changes introduce brand new features in the core part of the Bitcoin protocol. The limitations on the initial protocol were not moved (mostly*).

Drama and Threats

SV side

- #NoSplit
- “You split, we bankrupt you!”
- Reorg Attack Threads
- No Replay Protection
- Anti-Wormhole
- Government-Friendly
- Use Exclusive Licenses & Patents

- Most are Bitcoin Maximalists?

ABC side

- #CultOfCraig
- #Faketoshi
- Refusal to let miners vote on changes (as BU intended)
- Anti-Government
- Dislike Patents
- Anti-Reorg Checkpoints

- Most are OK with Multiple Coins?

Misconceptions

- Bitcoin SV is government controlled?
- Bitcoin SV miners will steal money from BCH users?
- Blocks bigger than 24MB are not possible at the moment?
- CSW wants to patent the Bitcoin Protocol and other already invented stuff?
- CSW patents are only valid on his chain?

- ABC team controls Bitcoin Cash?
- ABC wants Proof Of Stake, instead of PoW?
- BCH is illegal if it uses OP_DataSigVerify?
- Current BCH hashpower is Rented by Roger Ver?
- ABC supporters are also Ethereum supporters?

Which is the Real Bitcoin Cash

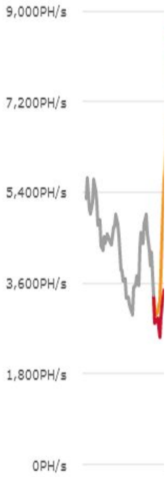
The Bitcoin ABC node implementation had a scheduled hard fork in it.
Basically - it was only usable till Nov 15 2018.

People had to Hard Fork.

ABC 0.18.* is a hard fork from ABC 0.17.*
SV   0.1.0   is a hard fork from ABC 0.17.*

The ABC version won the popular vote and kept the ticker symbol BCH
It also continued to exist after the split.
It is fair to say that BCH-ABC is Bitcoin Cash now.

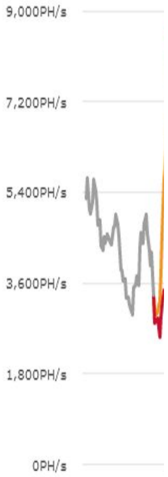
Hash War



- Before Sep 15 both sides were operating on the same chain.
- Miners were declaring which side they are taking by joining different mining pools.
- The SV side slowly grew.
  - From ~40% months before the fork
  - To ~85% days before the fork
- At that point BCH was consistently mined at a loss (relative to BTC)
- The SV side was tweeting “#NoSplit” stronger than ever
- The ABC side was framing this as a 51% attack on Bitcoin Cash

Hash War (#NoSplit)

The #NoSplit narrative was misunderstood.

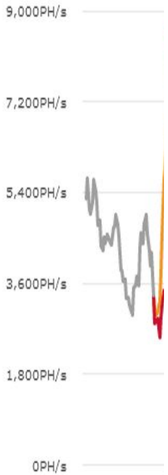


It was impossible to prevent a split.

- A split is permissionless
    - It only requires action from the ones who want to split.
- The forks were non-compatible
    - Technically, a split chain was inevitable.
    - Even if no one used the new OP codes, CTOR would ensure a split happened.
- The question wasn’t if there will be a split or not.
    - It was if both chains will exist long enough (to stabilize) after the split or 1 will prevail.

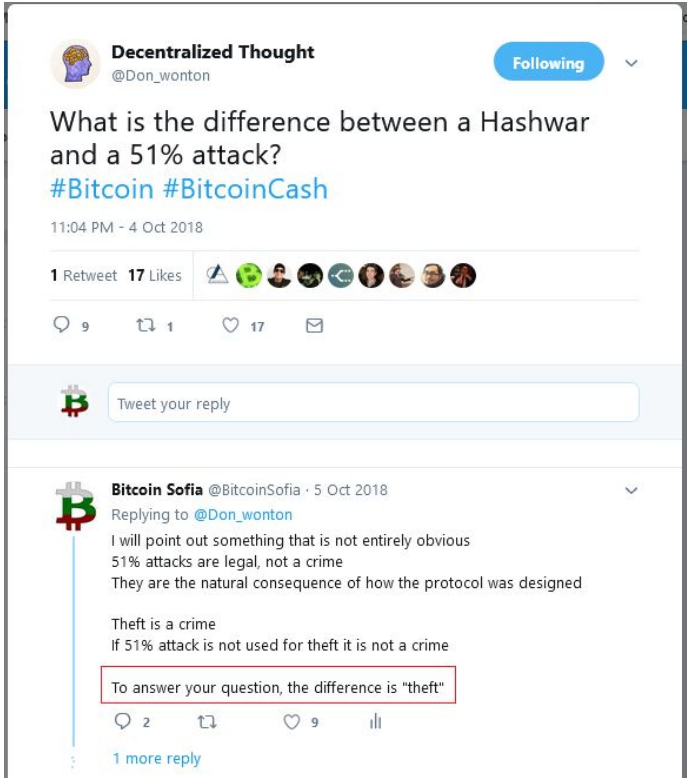
Hash War (Reorg Attacks)

Hash War between chains involves Reorg Attacks, but it is not a double spend attack.



- Double spend attack is attack on users.
  - The attacker buys something with coins but keeps the coins
  - Double spending is Theft

- Reorg Attack is an attack on the chain.
  - The attacker needs 51% of the chain's hashpower.
  - The attacker does NOT steal any money.
  - The attacker simply mines a longer chain than the honest miners.
    The blocks could contain the same TXs or be empty.
  - The honest miners lose the block reward they worked for.
    They worked for nothing.
  - The users do not lose money.
    Their transactions get replayed in the reorged chian.
  - Reorg Attacks are expensive.
  - Reorg Attacks are Not a Crime



Decentralized Thought
@Don_wonton

What is the difference between a Hashwar and a 51% attack?
#Bitcoin #BitcoinCash

11:04 PM - 4 Oct 2018

1 Retweet 17 Likes

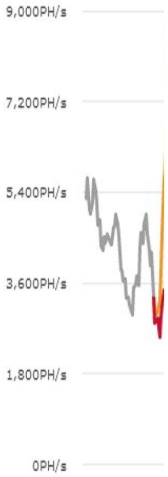
Bitcoin Sofia @BitcoinSofia · 5 Oct 2018
Replying to @Don_wonton
I will point out something that is not entirely obvious
51% attacks are legal, not a crime
They are the natural consequence of how the protocol was designed

Theft is a crime
If 51% attack is not used for theft it is not a crime

To answer your question, the difference is "theft"

Hash War (Reorg Attacks)

- Q: What to do when facing a reorg attack?



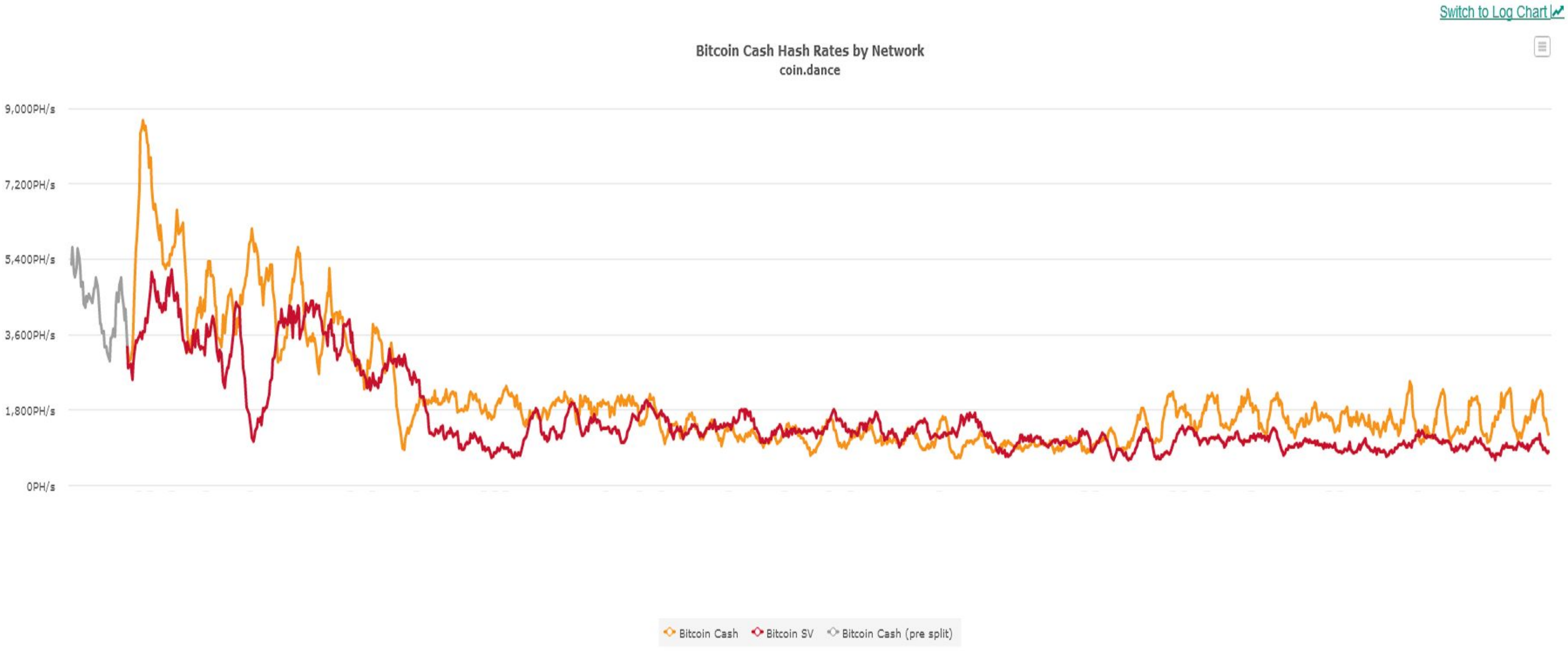
a. Buy more hashpower to make the attack harder.

b. Keep mining on the non-reorged chain at a loss, until you reorg the reorg.

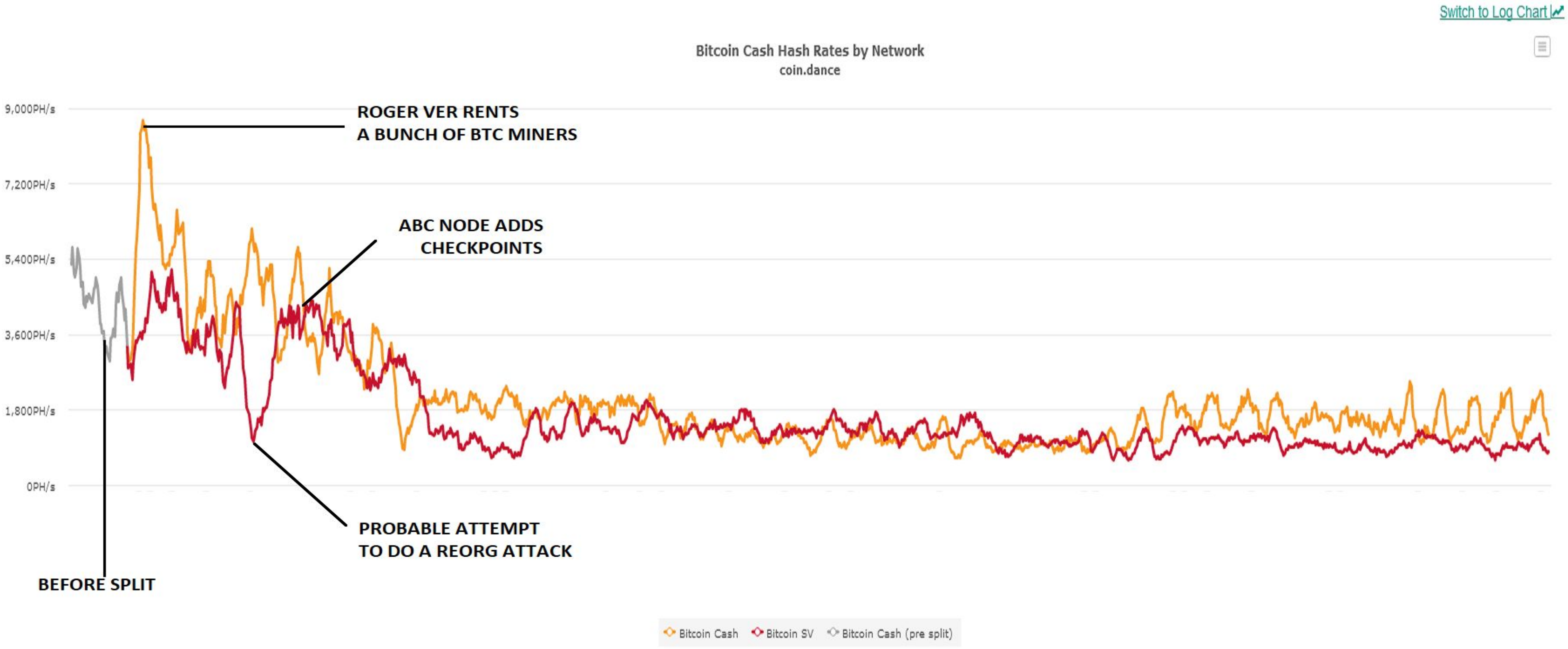
c. Give up and start mining on the new, reorged chain.

d. Update the node software to make other miners mine the non-reorged chain for you (by default), so that the mentioned above mining loss is socialized between all miners.

Hash War


Switch to Log Chart
Bitcoin Cash Hash Rates by Network
coin.dance
9,000PH/s
7,200PH/s
5,400PH/s
3,600PH/s
1,800PH/s
0PH/s
Bitcoin Cash
Bitcoin SV
Bitcoin Cash (pre split)

Hash War



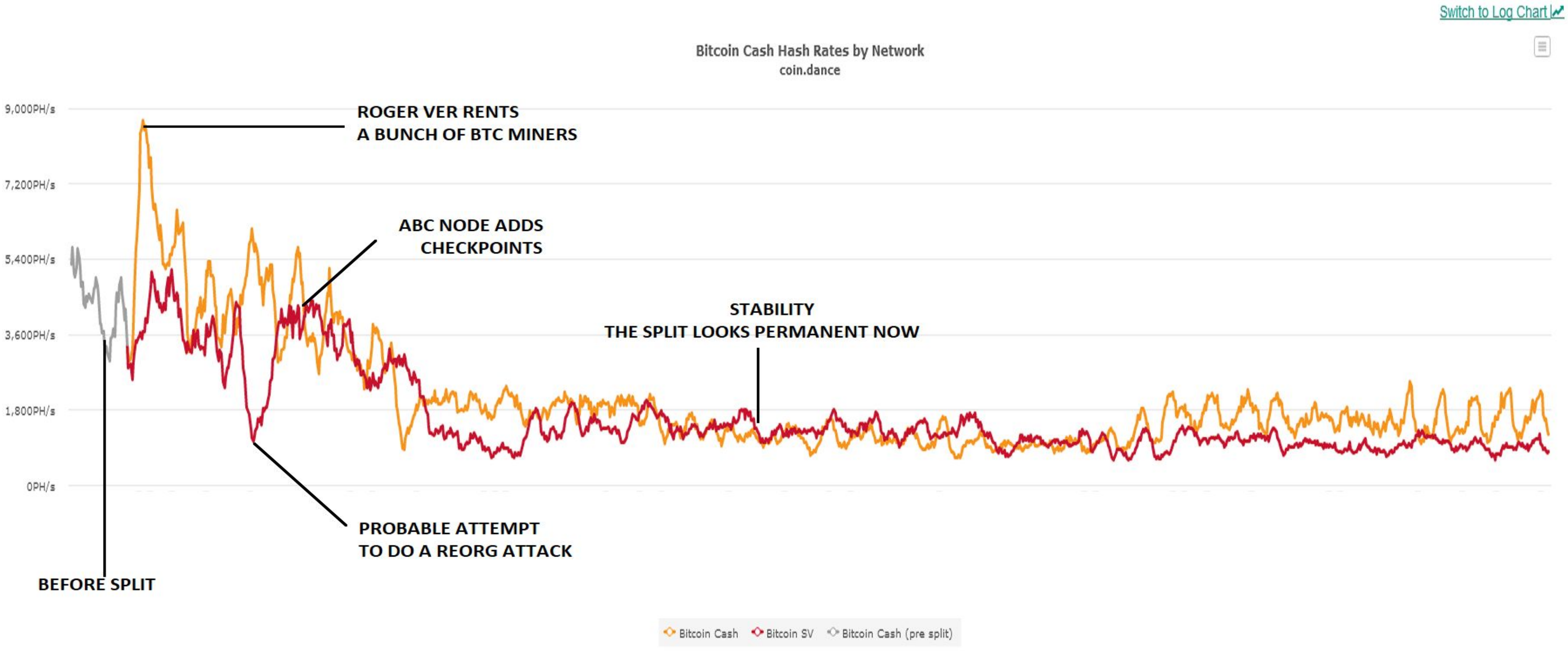
ROGER VER RENTS
A BUNCH OF BTC MINERS

ABC NODE ADDS
CHECKPOINTS

PROBABLE ATTEMPT
TO DO A REORG ATTACK

BEFORE SPLIT

Hash War



ROGER VER RENTS
A BUNCH OF BTC MINERS

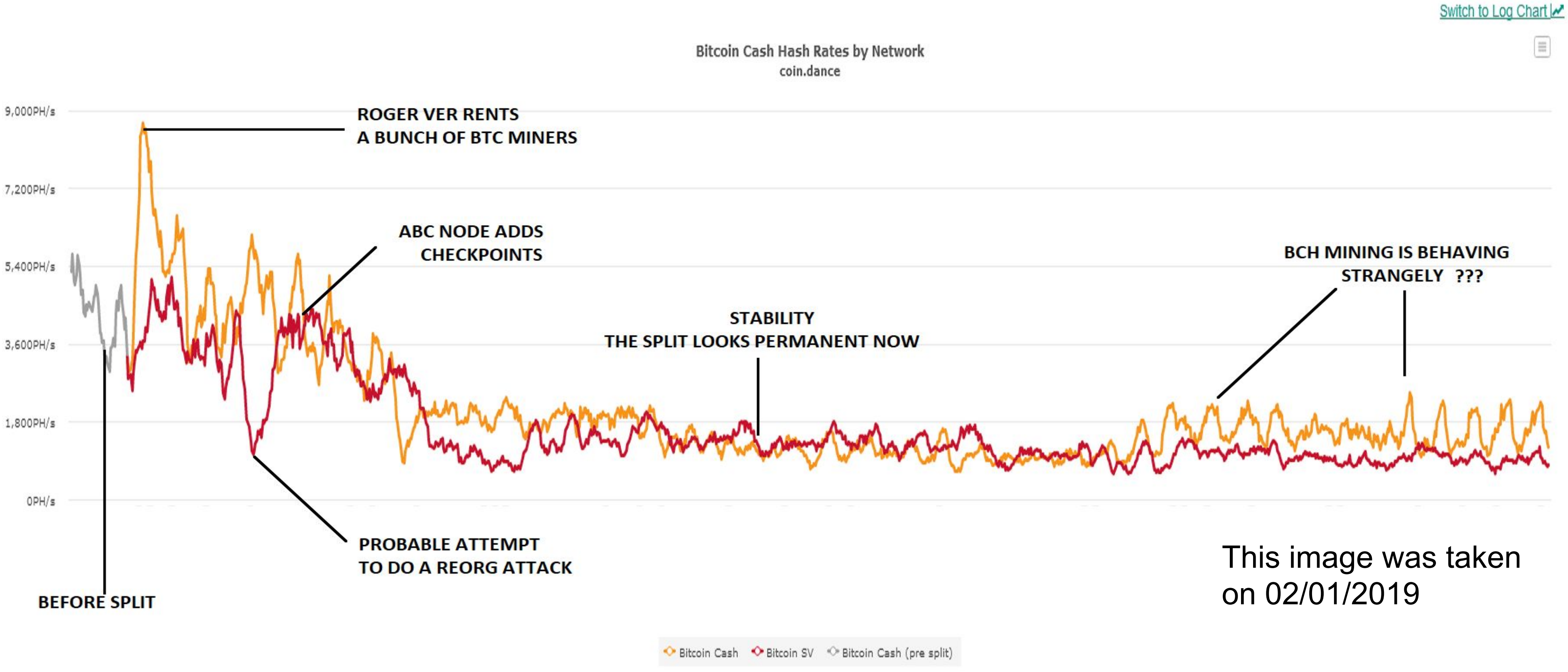
ABC NODE ADDS
CHECKPOINTS

STABILITY
THE SPLIT LOOKS PERMANENT NOW

PROBABLE ATTEMPT
TO DO A REORG ATTACK

BEFORE SPLIT

Hash War



ROGER VER RENTS
A BUNCH OF BTC MINERS

ABC NODE ADDS
CHECKPOINTS

STABILITY
THE SPLIT LOOKS PERMANENT NOW

BCH MINING IS BEHAVING
STRANGELY ???

PROBABLE ATTEMPT
TO DO A REORG ATTACK

BEFORE SPLIT

This image was taken
on 02/01/2019

Hash War

The hash war seems to be over.
BCH-ABC came on top!

ABC is now Bitcoin Cash.

Tribalism

- Millions of dollars were wasted in unprofitable mining.

- The price of both forked coins together is around half of the previous price.

- The community was divided into opposing tribes.

- Multiple projects chose to support only one of the sides, which ended up making both sides less usable.

- A Lawsuit were started.

Tribalism

- Q: Was all of that worth it?

- Q: Were the CTOR and DSV so terrible that the SV side had to go against them no matter what?

- Q: Were the benefits of CTOR and DSV so great that the ABC side had to implement them no matter what (even against the opinions of 80% of their miners)?

- I Don’t Know

Choice

I want to be a Proof Of Work maximalist.
I believe there will be only one PoW cryptocurrency chain.

I am also a fan of big blocks.
I believe the correct answer to global scaling of Bitcoin is big blocksize.

Choosing is hard :

Both [BCH] and [BSV] are **Proof of Work** networks that aim towards really **big blocks**.

Choice

Bitcoin SV promises:

- To increase the blocksize right now
- To remove script restrictions now
- To not change the protocol
- To be business friendly (stability)

- To be government friendly?

Bitcoin Cash promises:

- To increase the blocksize when the network is ready
- To remove script restrictions when the network is ready
- To make 0-conf secure with pre-consensus

- To be government independant?

Their approach to scaling is different, because their beliefs about how the world works are different.

Choice

Ultimately the choice between the two comes down to beliefs about **centralization**, miner **incentives** and **monopolies**.

- **Bitcoin Cash**

If one believes that **Bitcoin is broken** in the sense that miners are incentivised to seek to abuse their power, they'd want a more distributed system, where more people mine blocks on less expensive hardware.

- **Bitcoin SV**

If one believes that **Bitcoin works** in the sense that miners are incentivised to keep each other under control, they'd prefer to have bigger blocks right now and turn mining into a profession even if that makes it less distributed.

Choice

Is a choice necessary?

Not if:	
- **You want to use whatever is usable**	- Most people should be here
Maybe if:	
- **You want to build a business**	- If you are here, you know best
- **You want to HODL / gamble**	- Gamblers lose money!!
Yes if:	
- **You are a miner**	- I respect all PoW

My Choice

I chose SV.

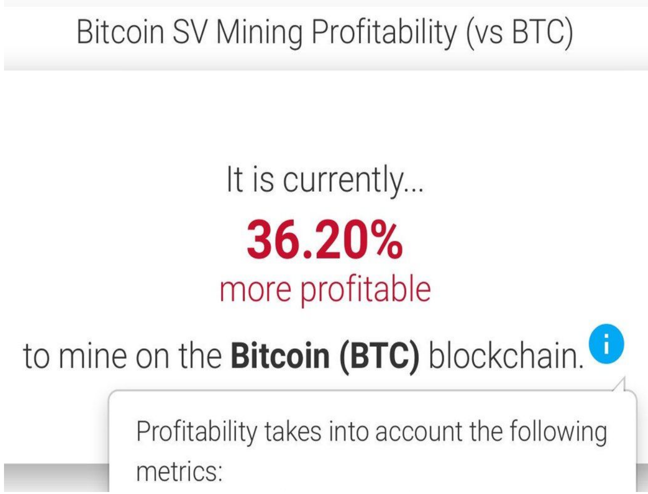
I believe Bitcoin Works.
I believe Big Blocks are the answer to scaling.

I made my choice as a holder. (Even if I don’t hold a lot.)
I made my choice as a business in the making. (see http://pipe.cash)

Something that really motivated me to make this choice was the **Proof of Work** that SV is doing.

This costs a lot of money.
I can not explain it, but **I can verify that it is real**.

(I believe it means that BSV miners value BSV more than the market does.)



Bitcoin SV Mining Profitability (vs BTC)

It is currently...

36.20%

more profitable

to mine on the **Bitcoin (BTC)** blockchain.

Profitability takes into account the following metrics:

Thank You

Do you have any questions?