Forks: What happened

12. December 2017

Daniel Pichler

Agenda

Types of Forks:

Orphans

Softfork

Hardfork

Tech of current Forks:

Ethereum Classic, Bitcoin Cash, Bitcoin Gold,...

Ideology Recap

Segwit / UASF/ NO2X 2017

About me

- Business, Psychology Undergrad
- Worked in Startup Community since 2013 - Pioneers.io
- MSc Data Science
- Board Member Bitcoin Austria (NGO)

@PichlerD

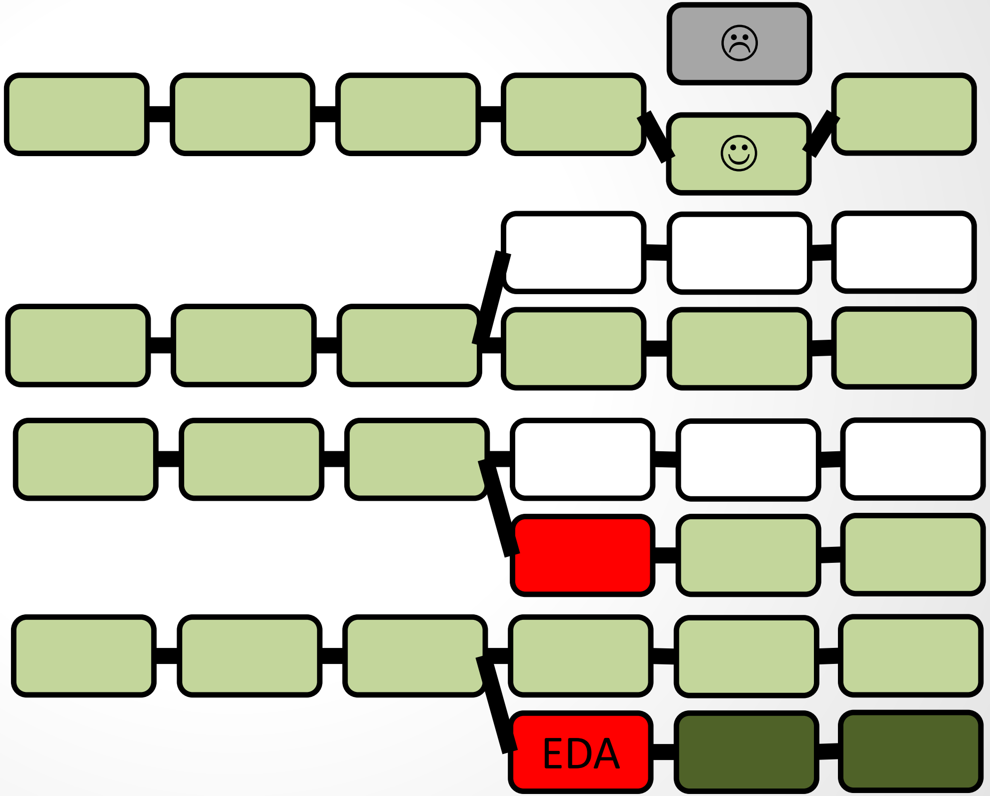
Types of Forks

‘Naturally’ occurring
e.g. Orphans

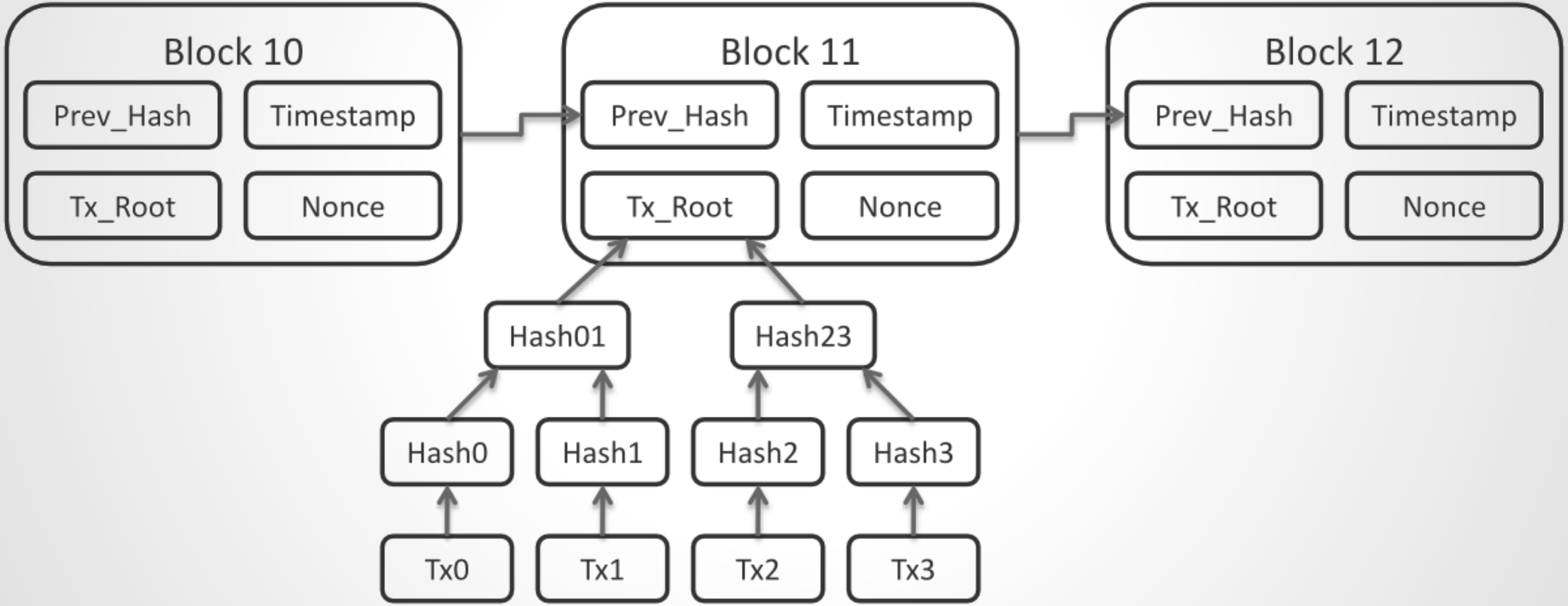
Soft Forks

Hard Fork with Majority

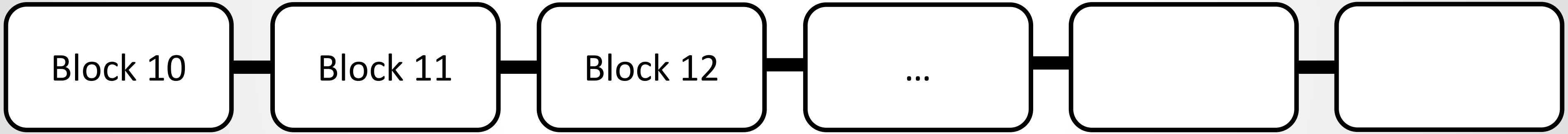
Hard Forks without Majority



Blockchain


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Blockchain



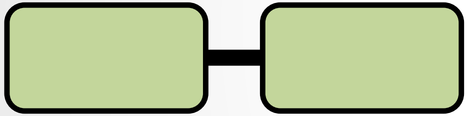
Block 10

Block 11

Block 12

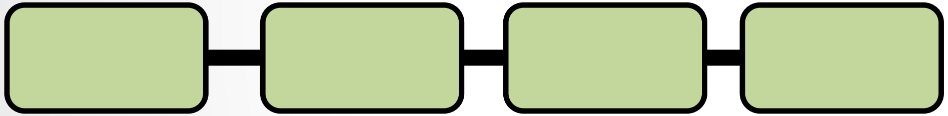
...

Unintentional forks

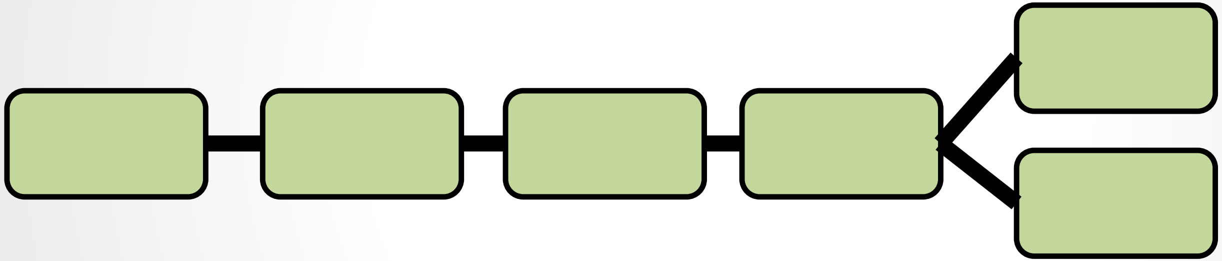


Unintentional forks

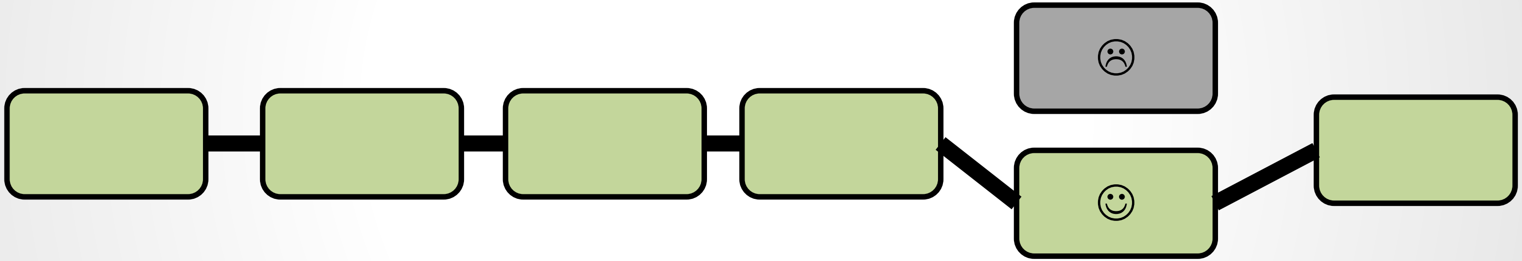
Unintentional forks



Unintentional forks



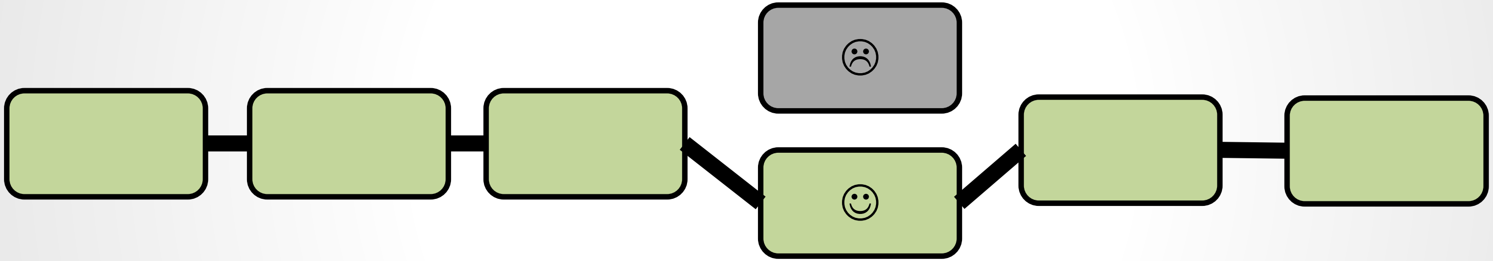
Unintentional forks



Grey Block was orphaned

Green Block continued and was further mined upon

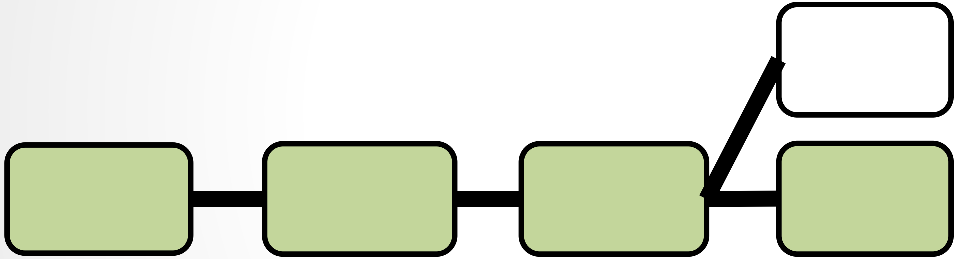
Unintentional forks



Happen unintentionally
Only split the blockchain temporarily
Shortly create two VALID blocks

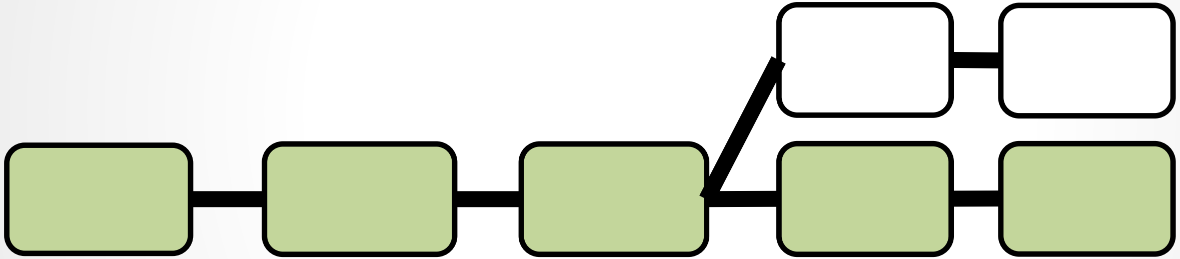
Soft Forks

Soft Forks



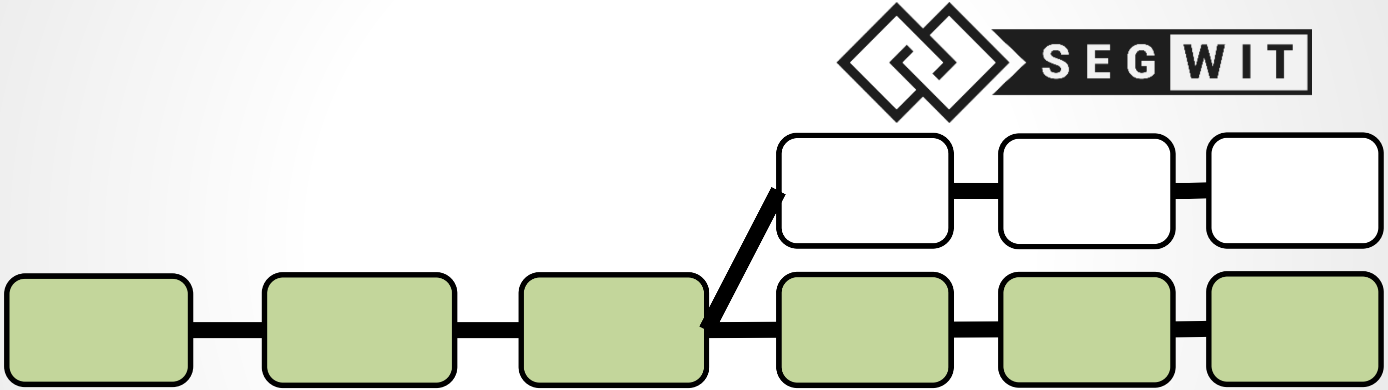
Green Blockchain still valid
Additional content in white addon

Soft Forks



Green Blockchain continuous to be VALID
Additional content in white addon

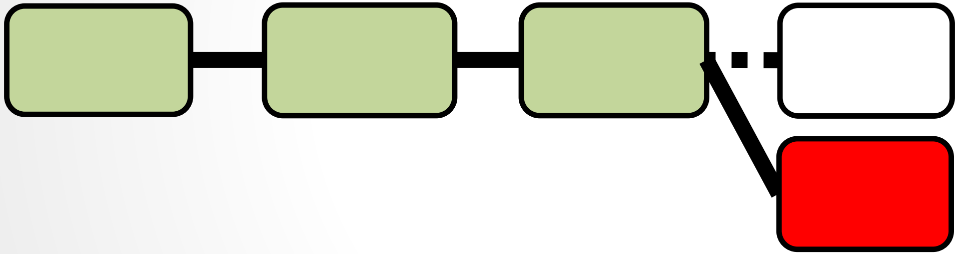
Soft Forks



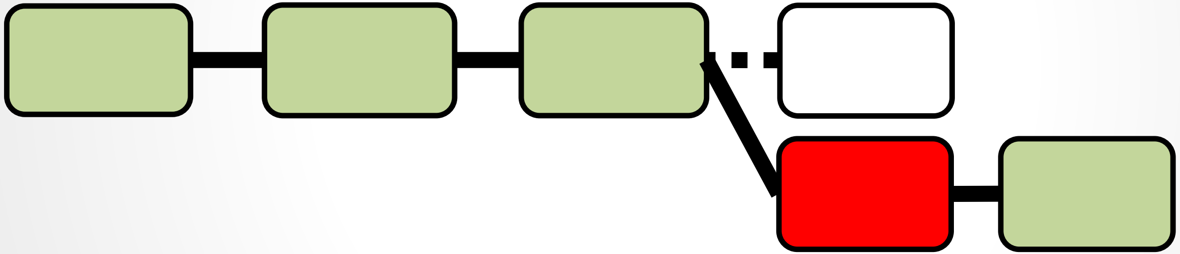
E.g. Segwit,
Downgrading Block Size Limit,
Non-rule changing changes

Majority Hard Fork Upgrade

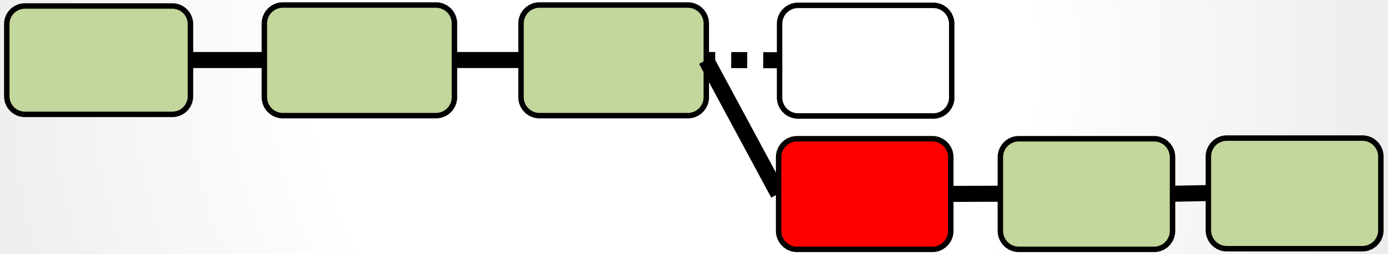
Majority Hard Fork Upgrade



Majority Hard Fork Upgrade



Majority Hard Fork Upgrade



Upgrades can happen through hard forks

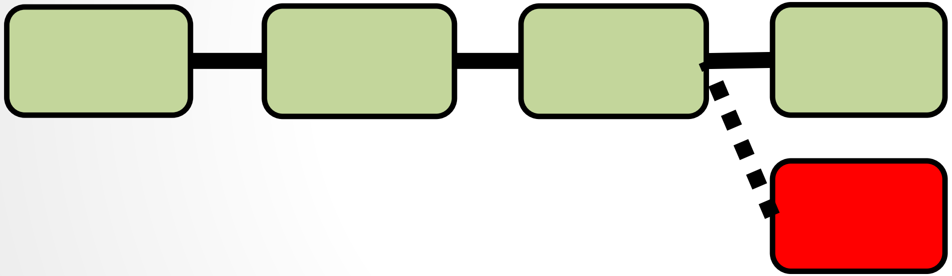
Solves e.g. major security flaws

August 2010, March 2013

Old Bitcoin Blockchain Dies as Difficulty is too high

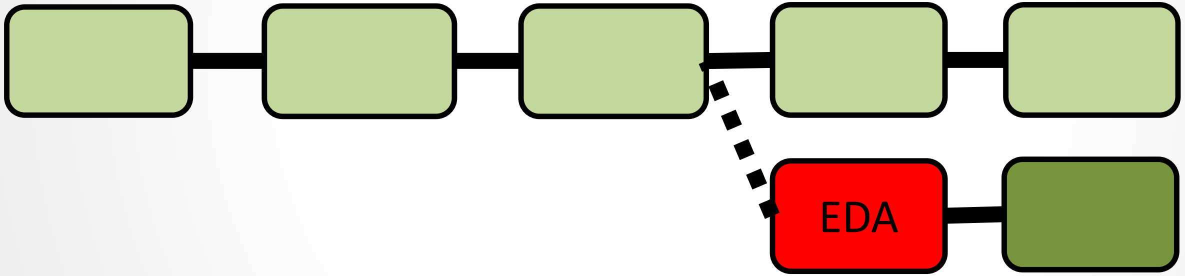
Minority Fork

Minority Fork



Creates a separate alive fork starting from same history

Minority Fork

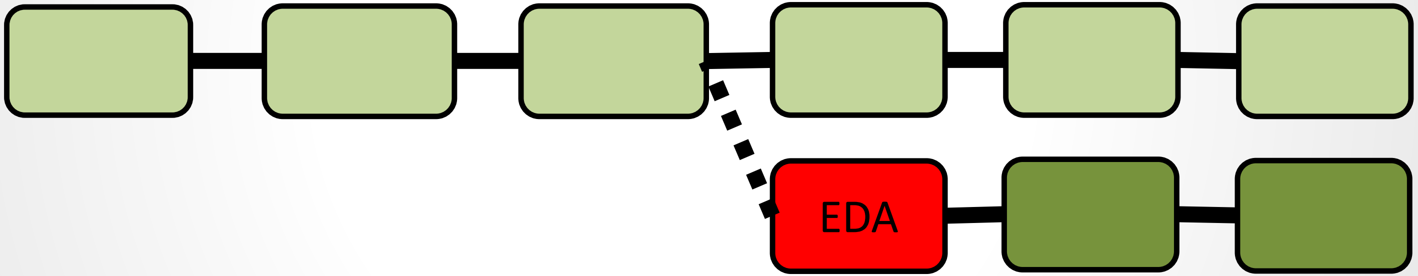


Has to keep minority alive or it will die due to non-profitability

Minority Fork

Bitcoin Cash

Peer-to-Peer Electronic Cash



Bitcoin Cash, Gold, Diamond are minority forks as they don’t have the majority of the hashing power during the hardfork

Types of Forks

Orphans

Happen unintentionally
Don’t split the blockchain permanently
Create VALID Blocks

Soft Forks

Don’t break the consensus algorithm but are intentional updates

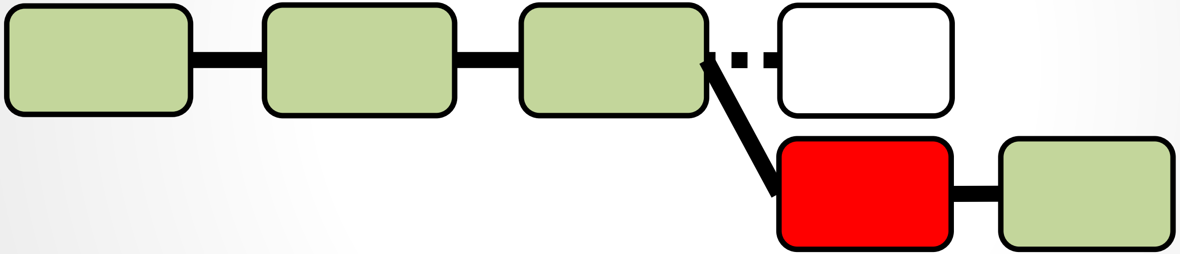
Majority Hard Fork

Major updates to a blockchain mostly for faulty reasons, can create a split of minority chain

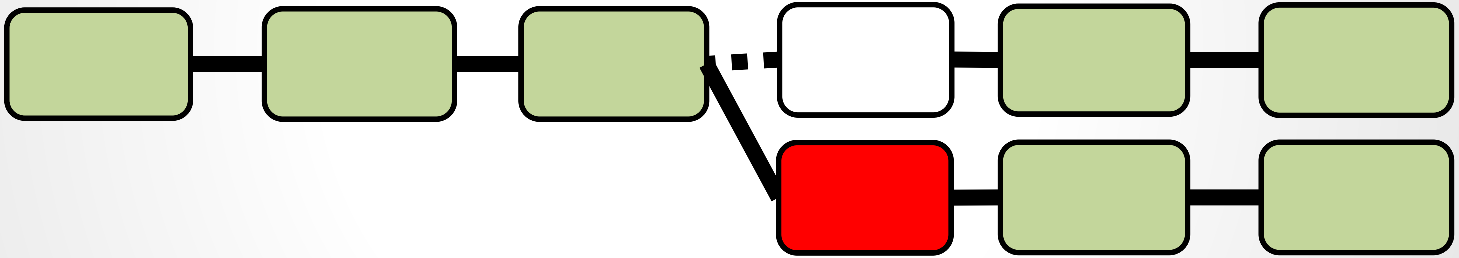
Minority Hard Fork

New coin spinoff that diverges technically from the old blockchain

Majority Hard Fork Upgrade



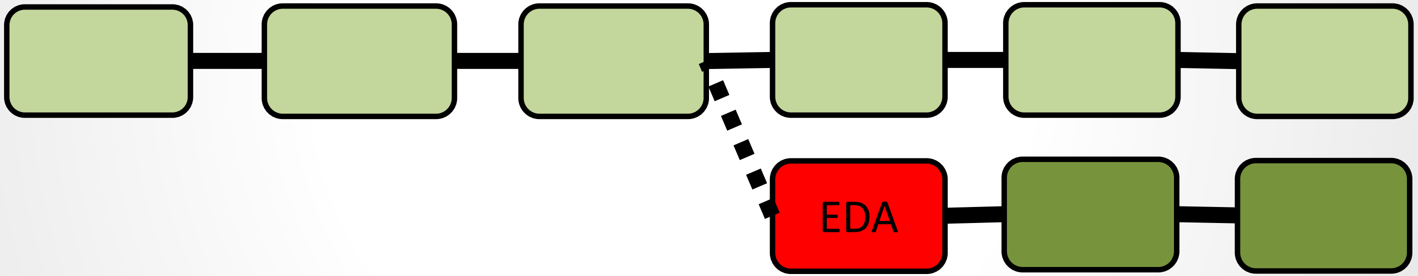
Ethereum Classic



Ethereum Classic came from a controversial Majority Hardfork Upgrade

As Ethereum has fast difficult adjustment it was possible to keep mining the old chain

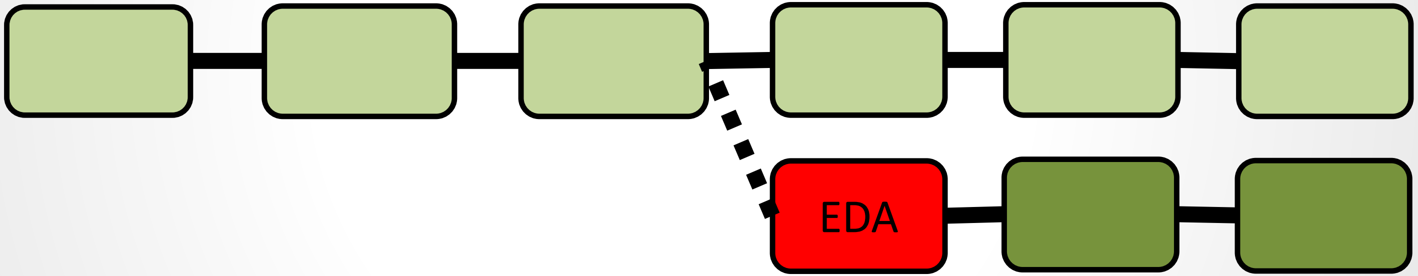
Minority Fork



Bitcoin Cash

Bitcoin Cash

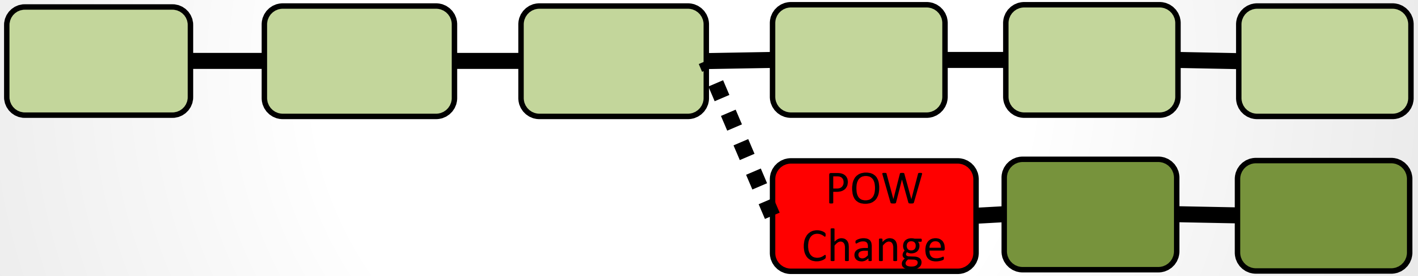
Peer-to-Peer Electronic Cash



Bitcoin Cash didn’t interfere with the Bitcoin Chain and created it’s own chain after a coordinated hard fork.

Hard Fork contained 2 changes – **Blocksize** and **Emergency Difficulty Adjustment** to keep the chain alive

Bitcoin Gold



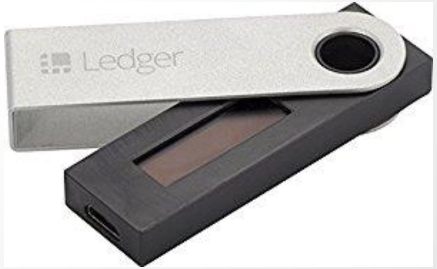
2 Changes:

200.000 Bitcoin Gold were given (pre-mined) to creators!

Mining Algorithm Change ZCash (Equihash) for GPU only mining

Your own addresses

- As it’s the same database, same amount contained in each address after fork (1:1)
- Replay protection necessary (Split tools)



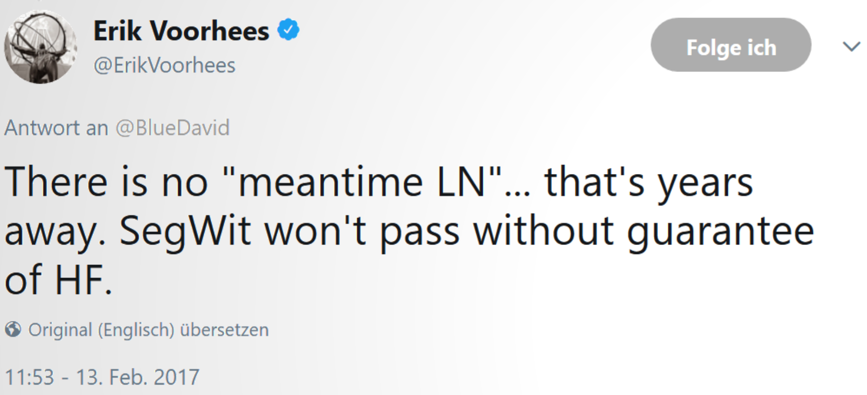
Custodial Wallets & Forks

- No legal obligations to give you forked coins
- Sometimes sell forks automatically
- Sometimes give forks very late
- E.g. Coinbase Bitcoin Cash 1st January

Airdrops

- Same rules apply for custodial/own wallets
- Have totally independent chain
- Give out free coins to spread them out in the market & promote themselves
- Sometimes proof is signature is needed

Segwit2x, NO2X



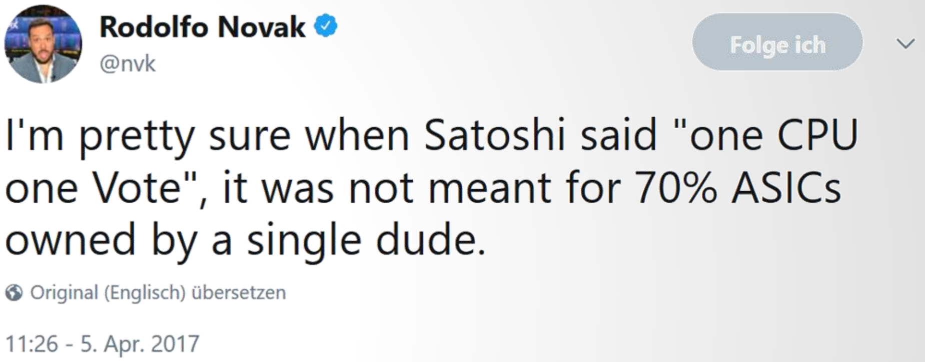
Erik Voorhees
@ErikVoorhees

Antwort an @BlueDavid

There is no "meantime LN"... that's years away. SegWit won't pass without guarantee of HF.

Original (Englisch) übersetzen

11:53 - 13. Feb. 2017

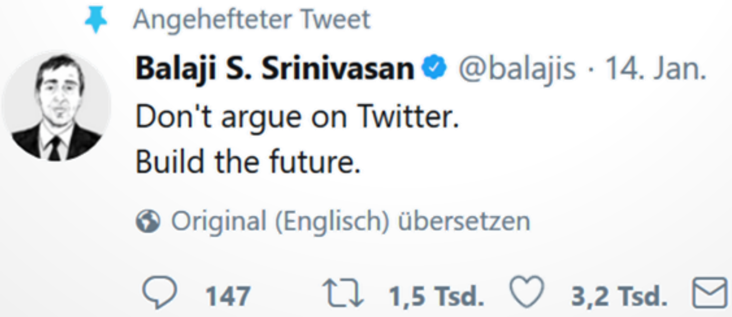


Rodolfo Novak
@nvk

I'm pretty sure when Satoshi said "one CPU one Vote", it was not meant for 70% ASICs owned by a single dude.

Original (Englisch) übersetzen

11:26 - 5. Apr. 2017



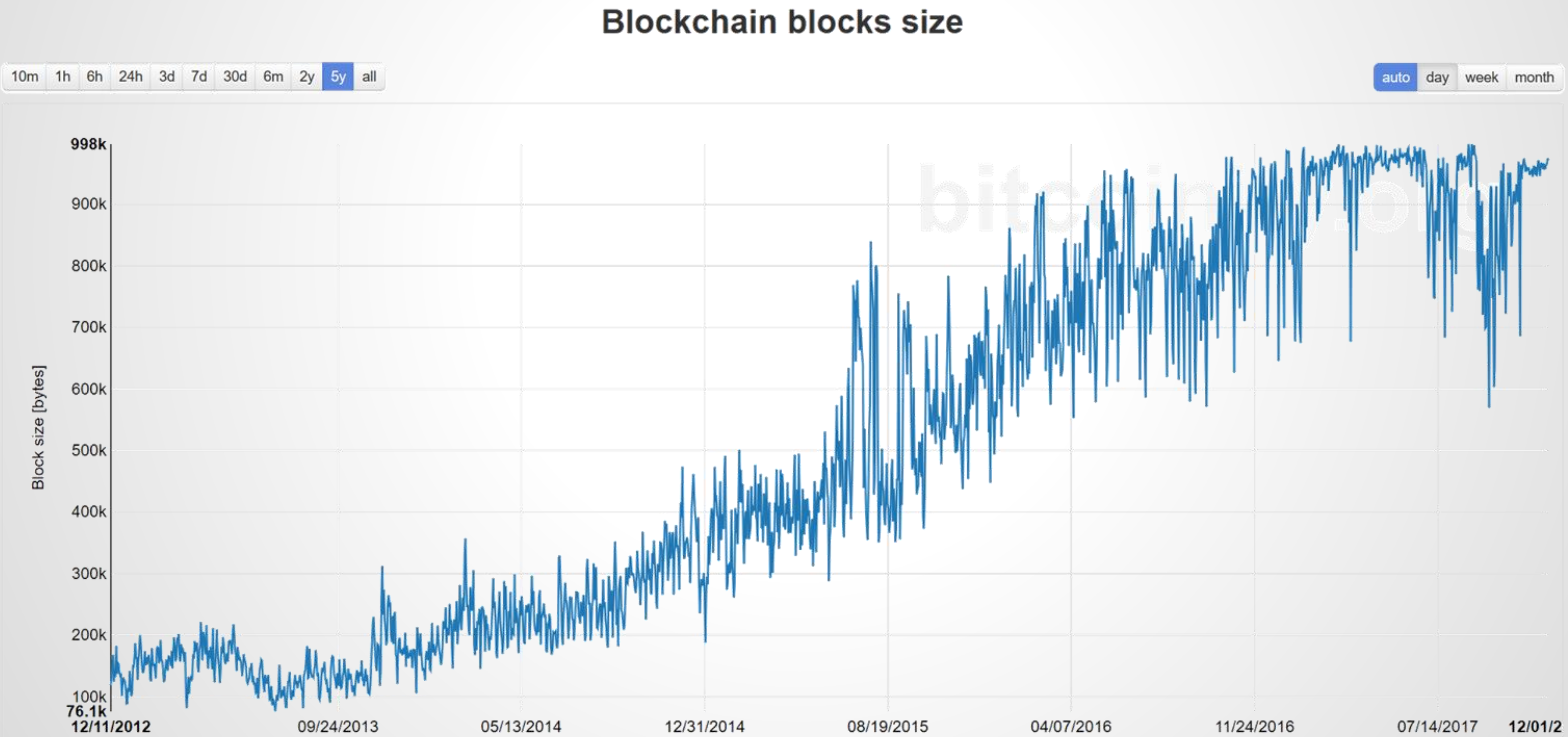
Angehefteter Tweet

Balaji S. Srinivasan @balajis · 14. Jan.

Don't argue on Twitter.
Build the future.

Original (Englisch) übersetzen

Bitcoin Cash/Gold
How did we get here?



Ideological Disagreement Timeline

2010

Giant Block was created - 1MB Blocksize limit soft-forked as spam control

2015

Gavin Andresen published BIP 101 (8MB)

2016

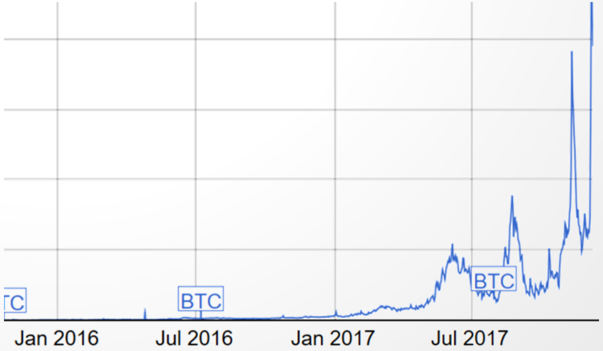
1MB limit hit first time – Transaction Fee & Altcoin Price Rising

2016

Segwit blocked by Miners to force Blocksize increase - UASF?

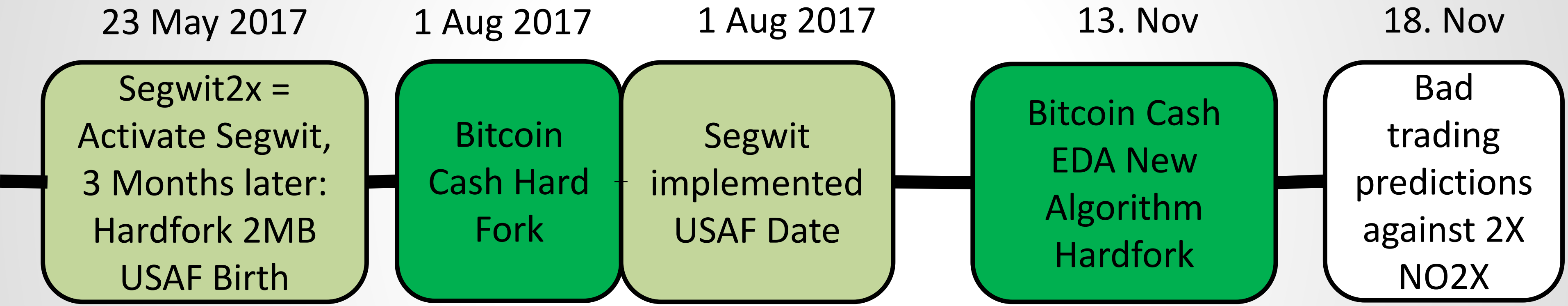
May 2017

Segwit2x Agreement



1Hash (China)
Abra (United States)
ANX (Hong Kong)
Bitangel.com /Chandler Guo (China)
BitClub Network (Hong Kong)
Bitcoin.com (St. Kitts & Nevis)
Bitex (Argentina)
bitFlyer (Japan)
Bitfury (United States)
Bitmain (China)
BitPay (United States)
BitPesa (Kenya)
BitOasis (United Arab Emirates)
Bitso (Mexico)
---Bitwala (Germany) BACKED OUT!
Bixin.com (China)
Blockchain (UK)
Bloq (United States)
btc.com (China)
BTCC (China)
BTC.TOP (China)
BTER.com (China)
Circle (United States)
Civic (United States)
Coinbase (United States)
Coins.ph (Phillipines)
CryptoFacilities (UK)
Decentral (Canada)
Digital Currency Group (United States)
---F2Pool (China) BACKED OUT!
Filament (United States)
Gavin Andresen (United States)
Genesis Global Trading (United States)
Genesis Mining (Hong Kong)
GoCoin (Isle of Man)
Grayscale Investments (United States)
Guy Corem (Israel)
Jaxx (Canada)
Korbit (South Korea)
Luno (Singapore)
MONI (Finland)
Netki (United States)
OB1 (United States)
Purse (United States)
Ripio (Argentina)
Safello (Sweden)
SFOX (United States)
ShapeShift (Switzerland)
surBTC (Chile)
Unocoin (India)
---*Vaultoro (Germany)*
Veem (United States)
ViaBTC (China)
---*Wayniloans (Argentina)*
Xapo (United States)
Yours (United States)

Ideological Disagreement Timeline



23 May 2017

Segwit2x = Activate Segwit, 3 Months later: Hardfork 2MB USAF Birth

1 Aug 2017

Bitcoin Cash Hard Fork

1 Aug 2017

Segwit implemented USAF Date

13. Nov

Bitcoin Cash EDA New Algorithm Hardfork

18. Nov

Bad trading predictions against 2X NO2X

Bitcoin Cash

Peer-to-Peer Electronic Cash

SEGWIT

Ideological Forks why?

Against high base fees

Bitcoin Cash

Peer-to-Peer Electronic Cash

Low Base layer Fees

No Segwit

8(32) MB Blocks possible

Gigablock Testnet

3rd biggest coin

Against central mining

BITCOINGOLD

1 GPU one vote

Equihash mining

Pre-mined

Segwit included

7th biggest coin

Bitcoin Cash
Peer-to-Peer Electronic Cash

bitcoin= austria

At that stage, most users should start running client-only software and **only the specialist server farms keep running full network nodes**, kind of like how the usenet network has consolidated.

If a **greedy attacker** is able to assemble more CPU proof-of-worker than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins

The steady addition of a constant of amount of new coins is analogous to **gold miners** expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

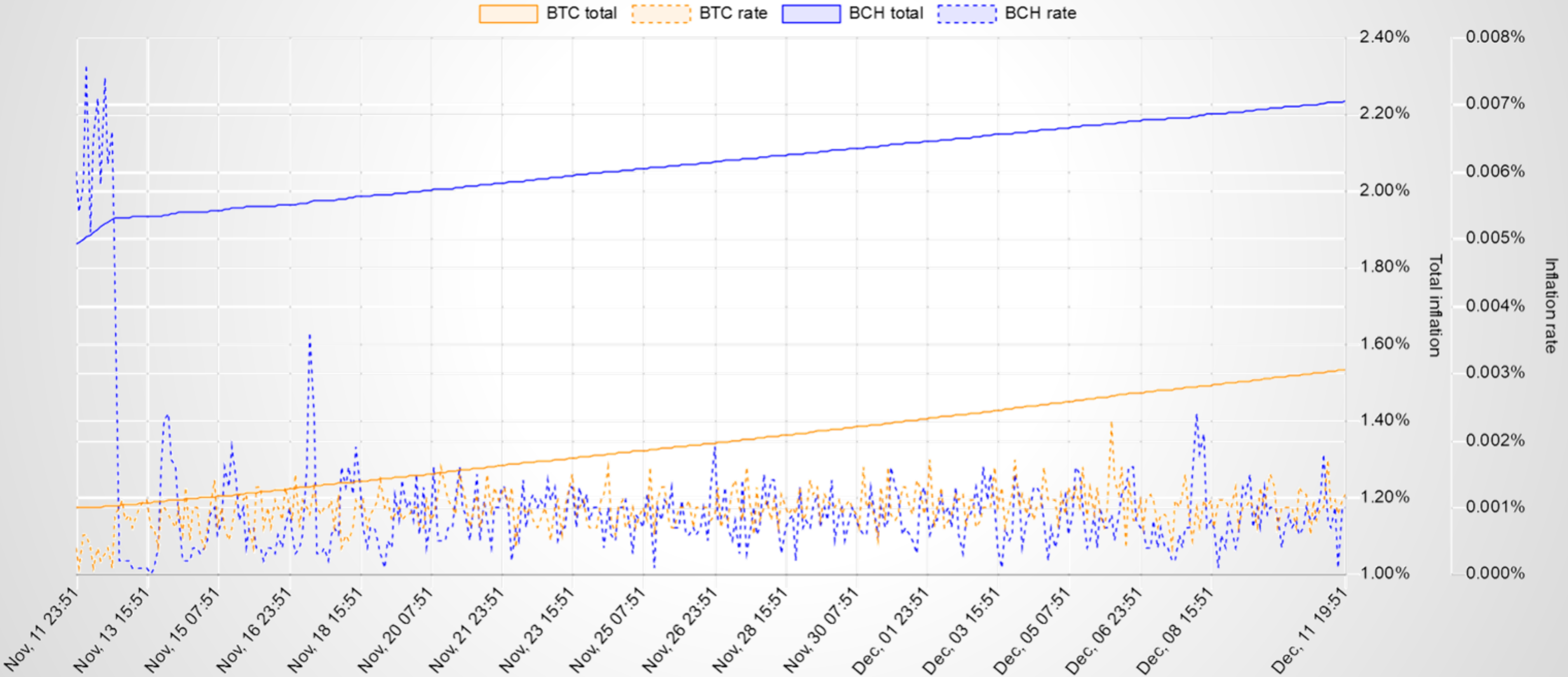
Proof-of-work is essentially ***one-CPU-one-vote*** – Satoshi

Chaindeath

Bitcoin/Bitcoin Cash? Friends or Foes?

- Bitcoin original chain can die if Bitcoin Cash price rises above Bitcoin’s price
- Spiral of sinking prices and slow difficulty adjustments would then never find enough blocks to adjust
- Bitcoin Cash has Emergency Difficulty Adjustment (EDA), saves it from destruction but causes higher inflation
- Bitcoin Cash has to take over Bitcoin rather sooner than later or will worsen it’s chances (Inflation!)

Inflation Rates



Monero December

RIAT - Institute for Future Cryptoeconomics

Neubaugasse 64-66/III/4 A-1070 Vienna,
Austria

riat.ac.at

Monero December is a focus-month, dedicated to Monero (http://monero.how/), a privacy-centric and securty-focussed cryptocurrency.

In December of 2017, the community and developers from the Monero project are invited to work,

present and develop in Vienna, Austria – hosted by RIAT.

Additionally, the time will be used to outline and plan the implementation of the Monero 34C3 Assembly

(https://events.ccc.de/congress/2017/wiki/index.php/Assembly:Monero_Assembly)

and combined other crypto/blockchain related assemblies at the CCC in Leipzig

(https://www.ccc.de/en/updates/2017/34C3-in-leipzig).

12. December 6 pm

65. Bitcoin Austria Meetup

Hardforks, Softforks

The 2x hardfork didn't take place, but others did, so… what actually is a fork?

Hardforks, Softforks, new coins, old coins. Let's talk about the tech and cryptoeconomics behind forks and understand what and why they are.

14. December 6 pm

Vienna (resurrected) Ruby Meetup

Bitcoin, Blockchain and Cryptocurrency

6 pm Welcome and reception

7 pm Opening Talk: Status of Ruby, Rails and an overview of Ruby 2.5

8 pm Status of Ruby & Cryptocurrency (Matthias Tarasiewicz)

8 pm Status and closer look on Ruby-Monero and Bitcoin-Ruby

9 pm Extensive overview of Ruby in Blockchain projects.

15. December 2 pm

Monero Meetup

Open Hardware Wallet, Traceability

2 pm Community hangout-start

6 pm Meetup start

6:30 pm Start and introduction to Monero (Matthias Tarasiewicz)

7 pm Input from the community: Overview of Monero Community Projects (live video-stream; sgp [tbc])

7:30 pm Bernhard Haslhofer (AIT) / Cryptocurrency Analytics beyond Bitcoin Crypto-Currency Analytics Plattforms in context of Monero / ZCash. http://bernhardhaslhofer.info

8 pm The Monero Open Source Hardware Wallet (msvb-lab)

16. December 7 pm

Free Code Camp Meetup

Workshops

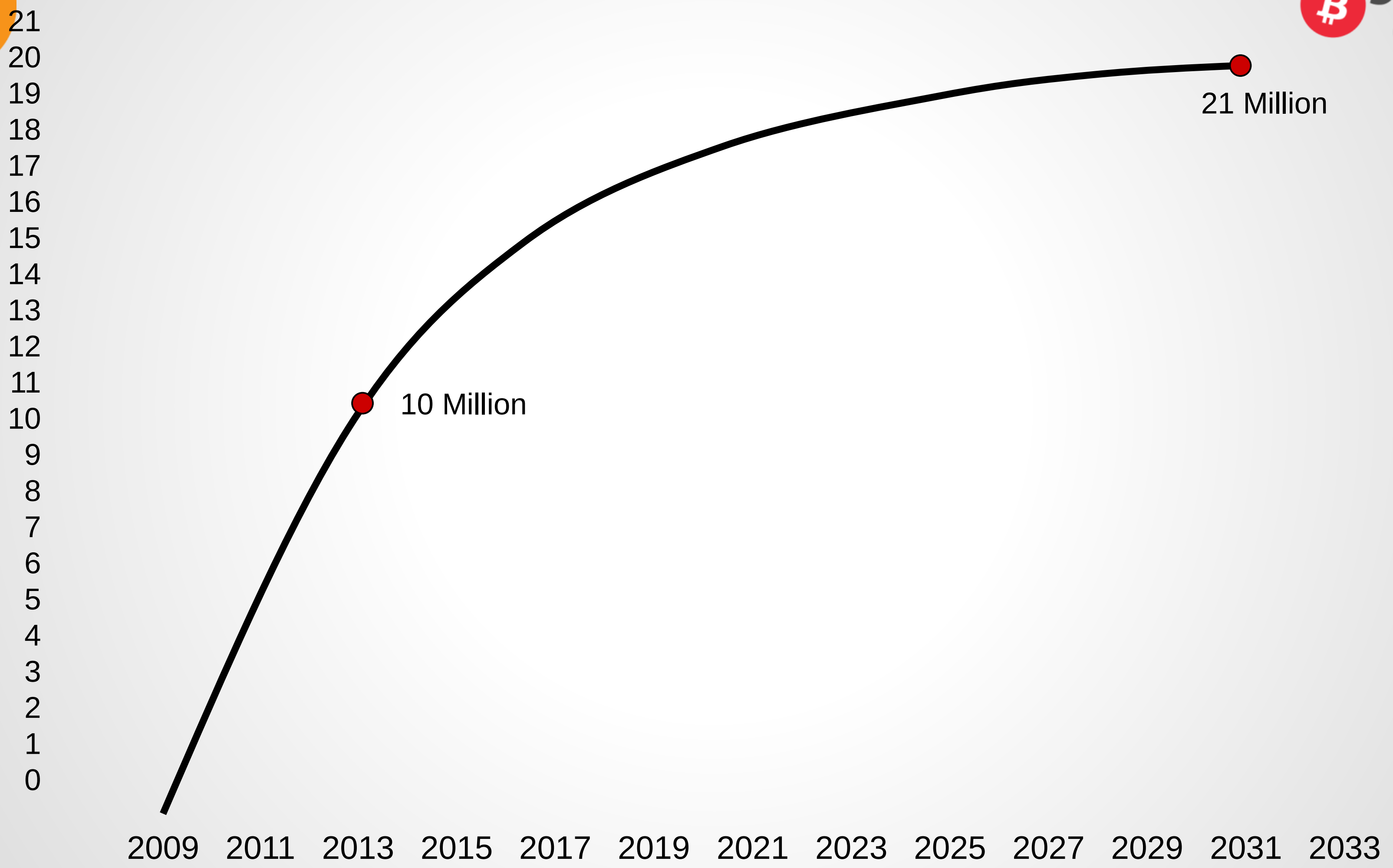
16. December 1 pm

Monero Open Hardware

Wallet Workshop (msvb-lab)

17. December 1 pm

Tomu.im 2FA development day


21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
10 Million
21 Million
2009
2011
2013
2015
2017
2019
2021
2023
2025
2027
2029
2031
2033