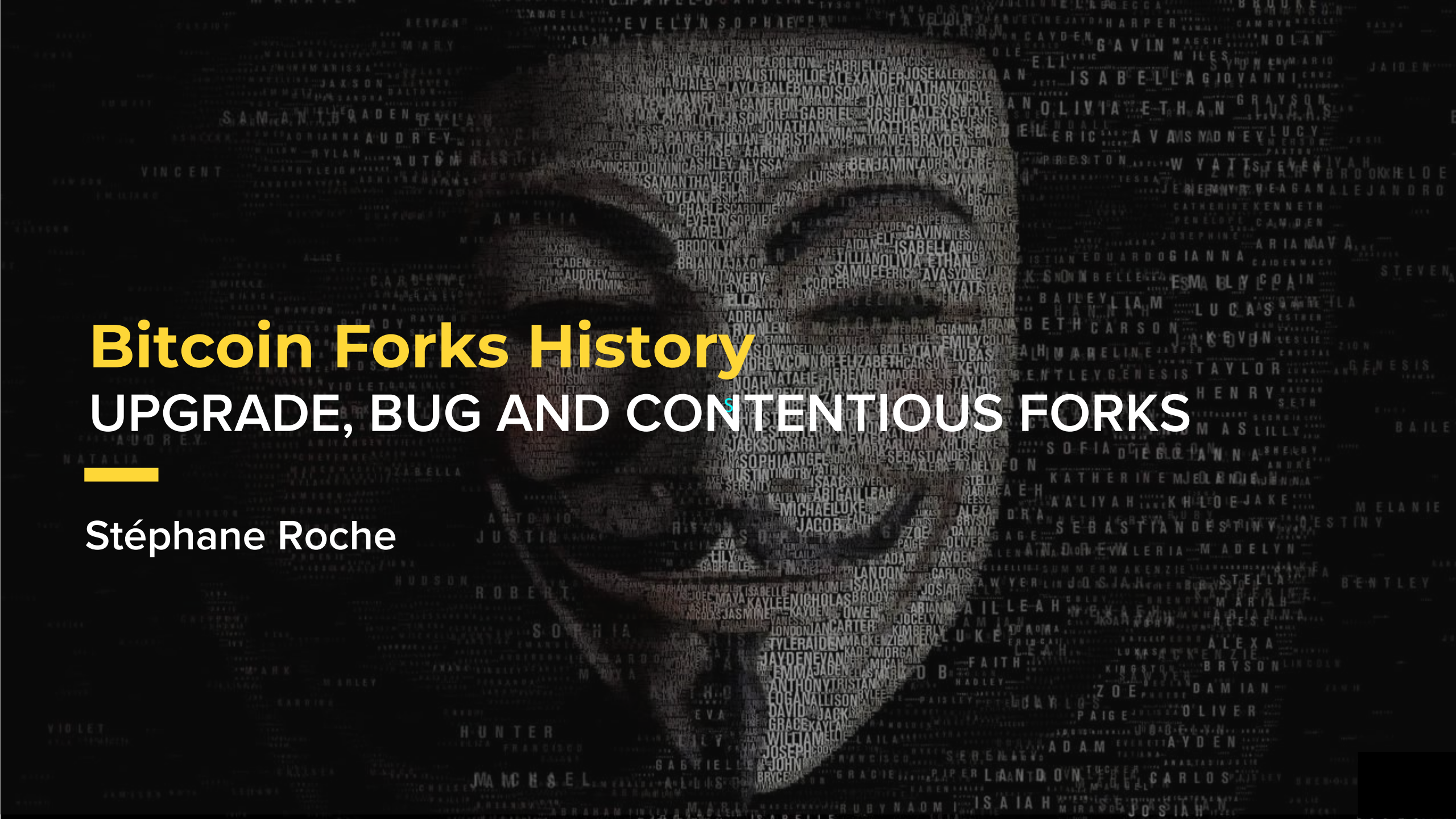


Bitcoin Forks History

UPGRADE, BUG AND CONTENTIOUS FORKS

Stéphane Roche

ABOUT STEPHANE

2015

Start working on Bitcoin in 2015 at Ledger (hardware wallet)

2016–2017

Work on Ethereum in 2016-2017

- Co-found non-profit organization Asseth
- R&D on Dao1901
- Contribute to the ERC20 Consensys smart contracts
- Dether.io (15,000 ETH raised)

2017–2018

Focus on blockchain technical trainings

Founder of D10eConsulting

Consultant at Chainsmiths

@janakaSteph on Twitter
rstephane@protonmail.com

OUTLINE

1. Main Consensus Forks
2. The Block Size Debate

1 MAIN CONSENSUS FORKS

- Bitcoin is a decentralized P2P consensus network
- A change to the consensus rules = fork
- 18 consensus rule changes to date
- Protocol upgrade is an active field of research
  - Since now, it has been trial and errors
  - Exploring new protocol upgrade methods
  - Lot of forks post-BCH can teach us a lot
  - Still not trivial at all

BIP-123 OFFICIAL FORKS TAXONOMY

Soft Forks

- Some [cryptographic commitment] structures that were valid under the old rules are no longer valid under the new rules
- Structures that were invalid under the old rules continue to be invalid under the new rules

Hard Forks

- Structures that were invalid under the old rules become valid under the new rules

SF ACTIVATION METHODOLOGY PHASES

- The 2010 forks: No activation methodology
- The 2012 forks: Towards a methodology
- March 2013 – December 2015: BIP34 versioning aka IsSuperMajority
- December 2015 – July 2017: Version bits (BIP9)
- July 2017 – August 2017: SegWit activation drama
- Next one in BIP-8 ?

THE 2010 FORKS: NO ACTIVATION METHODOLOGY

28 July 2010	0.3.5	OP_RETURN disabled. Fixing a critical bug which enabled anyone to spend any Bitcoin	No evidence of any issues
31 July 2010	0.3.6	OP_VER and OP_VERIF disabled	Some users had trouble upgrading S.N. recommends to shutdown nodes
		The addition of the OP_NOP functions	
01 Aug 2010	0.3.7	Separation of the evaluation of the scriptSig and scriptPubKey. Fixing a critical bug which enabled anyone to spend any Bitcoin	No evidence of any issues
15 Aug 2010	0.3.10	Output value overflow bug fix following a 184.5 billion Bitcoin spend incident	Chainsplit during 51 blocks. Fix released after 5h
		Disabling OP_CAT, which removed a DoS vector, along with the disabling of 14 other functions	
07 Sept 2010	0.3.12	Adding the 20,000 signature operation limit, in an incorrect way. This incorrect limit still exists today	No evidence of any issues
12 Sept 2010	n/a	Adding the 1MB blocksize limit	No evidence of any issues

2012: TOWARDS A METHODOLOGY

- BIP-30 (require tx to have a unique identifier)
  - Applied to all blocks whose timestamp is after March 15, 2012, 00:00 UTC
  - Simple flag day activation because the only way for a miner to violate it was to forever destroy 50 BTC by reusing a scriptpubkey in a coinbase output

- BIP-16 (P2SH)
  - 55% activation threshold, over blocks in the 7 days prior to 1 February 2012
  - Miners did not upgrade fast enough, so the evaluation point was delayed until 15 March

BIP-34 VERSIONING AKA ISSUPERMAJORITY

- First mechanism that employed hashpower activation
  - Requires trusting the hashpower will validate after activation

- 75% threshold signaling within a 1000 block interval to enforce the new rule
- Once 95% of blocks had the higher version, blocks with the lower version number would be rejected

- Version 2 (BIP34) – March 2013
- Version 3 (Strict DER encoding – BIP66) – July 2015
- Version 4 (CheckLockTimeVerify – BIP65) – December 2015

BIP-66 DEPLOYMENT INCIDENT

- Some non-upgraded miners (from the remainaning 5%) generate invalid blocks
- Roughly half the network hashrate was mining without fully validating blocks (SPV mining), and built new blocks on top of that invalid block
- The soft fork caused two chain splits (during 6 and 3 blocks)
- Consequences:
  - Miners lost funds
  - Some softwares don’t detect invalid blocks
  - Network unreliability (ask for 30 extra confirmations)

ISM LIMITATIONS

- Soft forks could only be deployed one at a time
- Miners can signal without really validating and enforcing
- If any activation failed for whatever reason, it would prevent any further soft forks from being deployed and activated

BIP-9 AKA BETTER VERSIONING

- Allow parallel soft fork deployment
  - Use different bits in the version field for each soft fork rather than increasing the version number
  - Up to 29 soft forks parallel deployment, activated independently
- Still rely on hashpower signaling
- Used for the relative timelocks functionality
  - CheckSequenceVerify (BIPs 68, 112, 113)

SEGREGATED WITNESS ACTIVATION DRAMA

- SegWit soft fork (BIPs 141, 143, 147) became highly politicized
- Threats of running other versions of Bitcoin software (UASF, Cash, 2X)
- Divergence of interest between miners and economic majority
- Majority of hashpower refused to signal until last minute

BITCOIN CORE PROPONENTS FIGHT BACK

- BIP-91 (Reduced threshold Segwit MASF) – 23 July 2017
  - Network rejects the non-signaling blocks
  - Pressure to force SegWit with current deployment method

- BIP-148 (Mandatory activation of segwit deployment) – 01 August 2017
  - Mix of BIP-9 MASF and UASF
  - Goal is to align miners and users interests
  - Incentivizing miners to work for the economic majority
  - Means of pressure to activating SegWit early

- BIP-8 (Version bits with lock-in by height) - proposed on February 2017
  - Alteration to BIP-9 that replaces time based activation with block height, as well as guaranteed activation of soft fork

HTTPS://BITCOINUASF.ORG/

Download Bitcoin Core with BIP148 support

Latest version: 0.14.2-uasfsegwit1.0

Choose your operating system

Windows
64 bit - 32 bit

Linux (tgz)
64 bit - 32 bit

Windows (zip)
64 bit - 32 bit

ARM Linux
64 bit - 32 bit

Mac OS X
dmg - tar.gz

Ubuntu (PPA)

Verify release signatures

Source code

Signing Keys

Luke Wladimir

LESSONS LEARNED

- Instrumentalization of the MASF deployment mechanism
  - 95% was chosen just to be on the safe side. Never intended to be a *vote*

- Too much responsibilities granted to miners => risk of veto

- Signalling mechanism ≠ enforcement of rules (cf. BIP-66)

2

BLOCK SIZE DEBATE


BITCOIN UNLIMITED PRESENTS
SATOSHI'S VISION
23-25 MARCH 2018
TOKYO JAPAN
SPONSORED BY
Bitcoin.com
BITMAIN
learn more

DEVELOPING THE PROTOCOL

AMAURY SÉCHET
LEAD DEVELOPER,
BITCOIN ABC

ANDREW STONE
LEAD DEVELOPER,
BITCOIN UNLIMITED

TOM HARDING
LEAD DEVELOPER,
BITCOIN XT

BUILDING THE PERMISSIONSLESS ECONOMY

RYAN X. CHARLES
CO-FOUNDER AND CEO,
YOURS.ORG

ROB DANIELSON
CO-FOUNDER,
ROCKETR.NET

CHRIS PACIA
DEVELOPER,
OPEN BAZAAR

RESEARCHING FOR THE FUTURE

PETER RIZUN
CHIEF SCIENTIST,
BITCOIN UNLIMITED

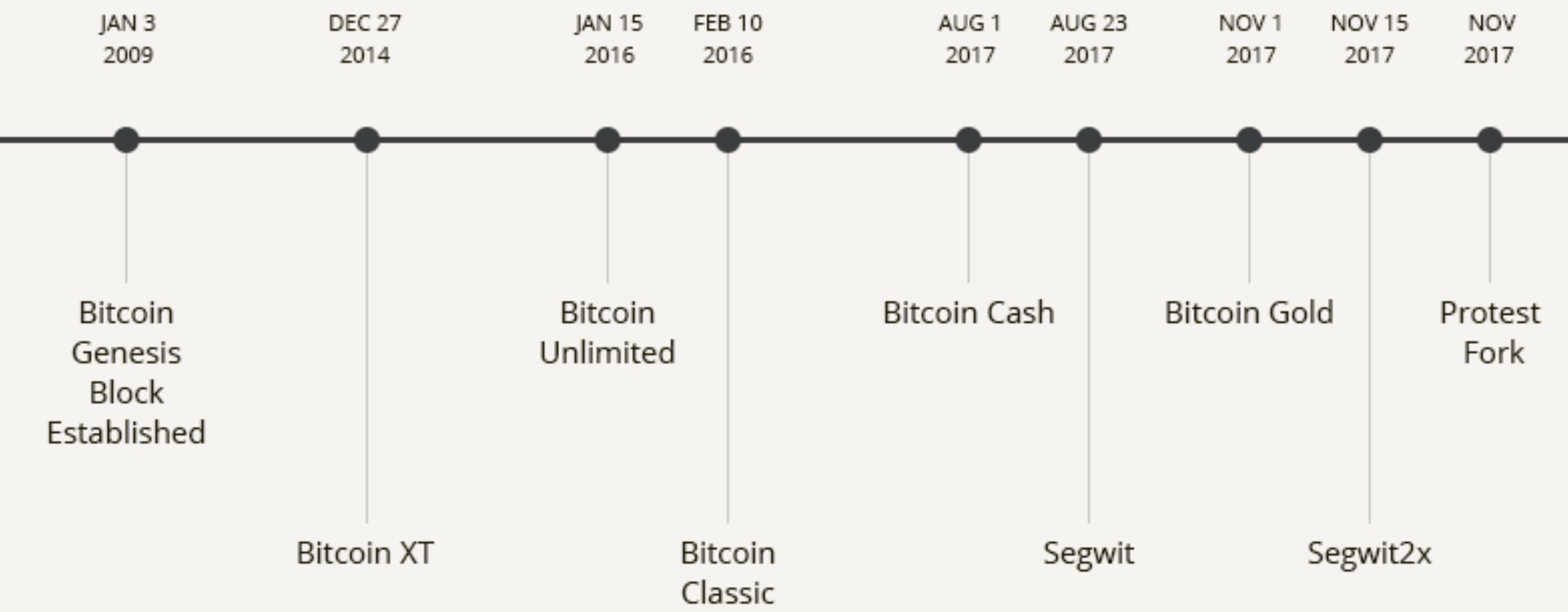
EMIN GÜN SIRER
ASSOCIATE PROFESSOR,
CORNELL UNIVERSITY

JOANNES VERMOREL
FOUNDER, LOKAD

THE BLOCK SIZE DEBATE

- A size issue: Small blockers vs Big blockers
- Lot of alternative implementations for bigger blocks
- While Bitcoin Core is focusing on optimization and layer 2

Bitcoin Forks Timeline



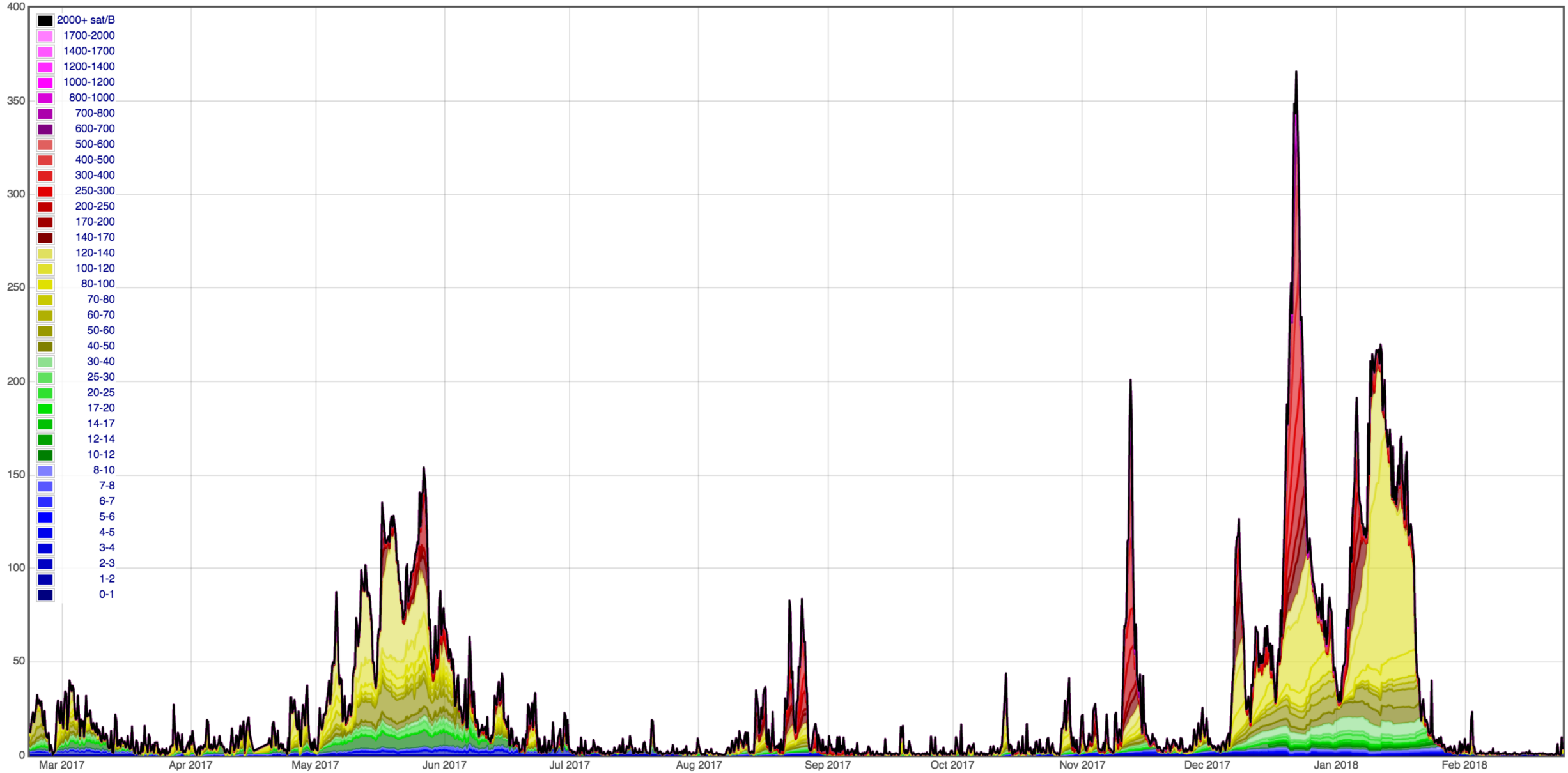
BITCOIN CORE ROADMAP

- 1MB block size limit

- Optimization rather than bigger block
  - libsecp256k1 verification (500% to 700% speed boost on x86_64)
  - Block compression (IBLT, Weak Block, Compact Block, ...)
  - Segregated Witness (up to x4)
  - Schnorr signatures
  - ...

- Off-chain overlay network (layer 2)
  - Lightning Network

Pending Transaction Fee in BTC

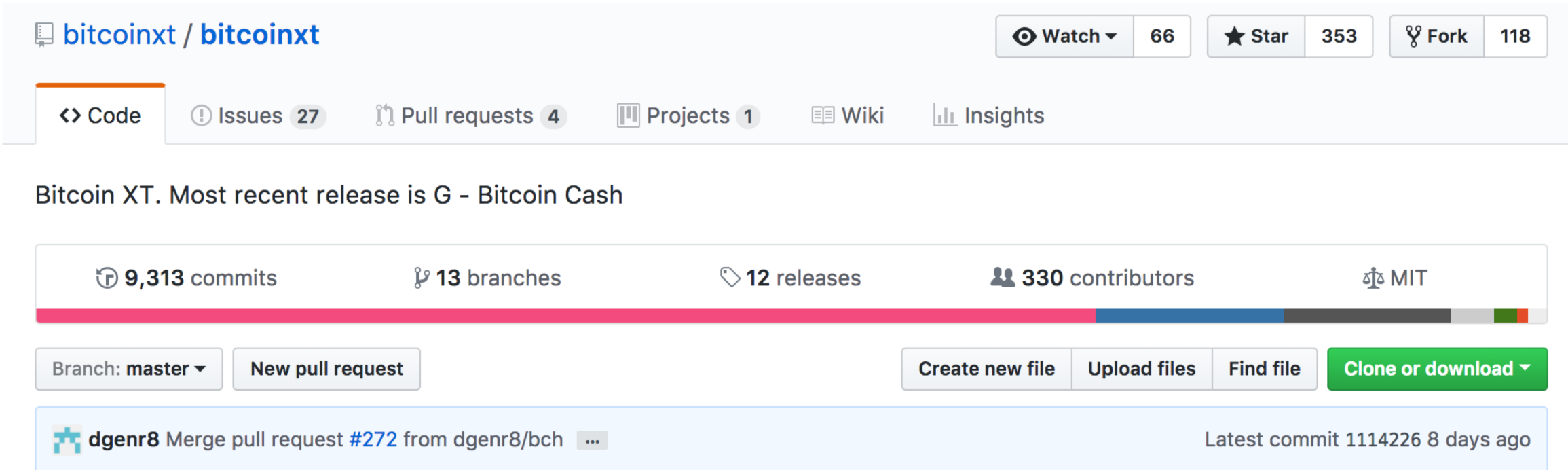


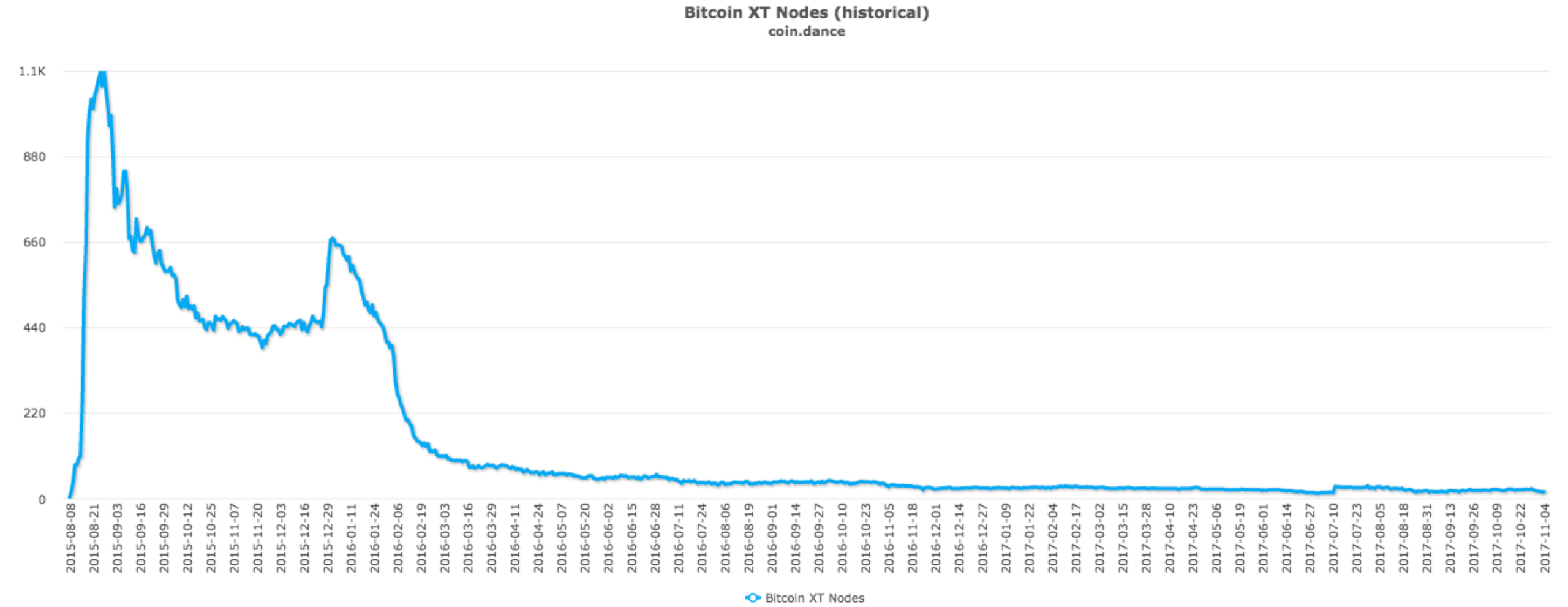
BITCOIN XT IMPLEMENTATION

- Dec 2014: First client launched by Mike Hearn
- Jun 2015: Plan to increase the max block size (BIP0101)
  - Max block size increase to 8MB, doubling every two years
  - Aug 2015: BIP 101 merged into the XT codebase
  - 75% hashrate threshold never met
  - Jan 2016: BIP 101 reverted and 2MB block size of Bitcoin Classic applied instead
- Now defaults to being a Bitcoin Cash client

Bitcoin XT

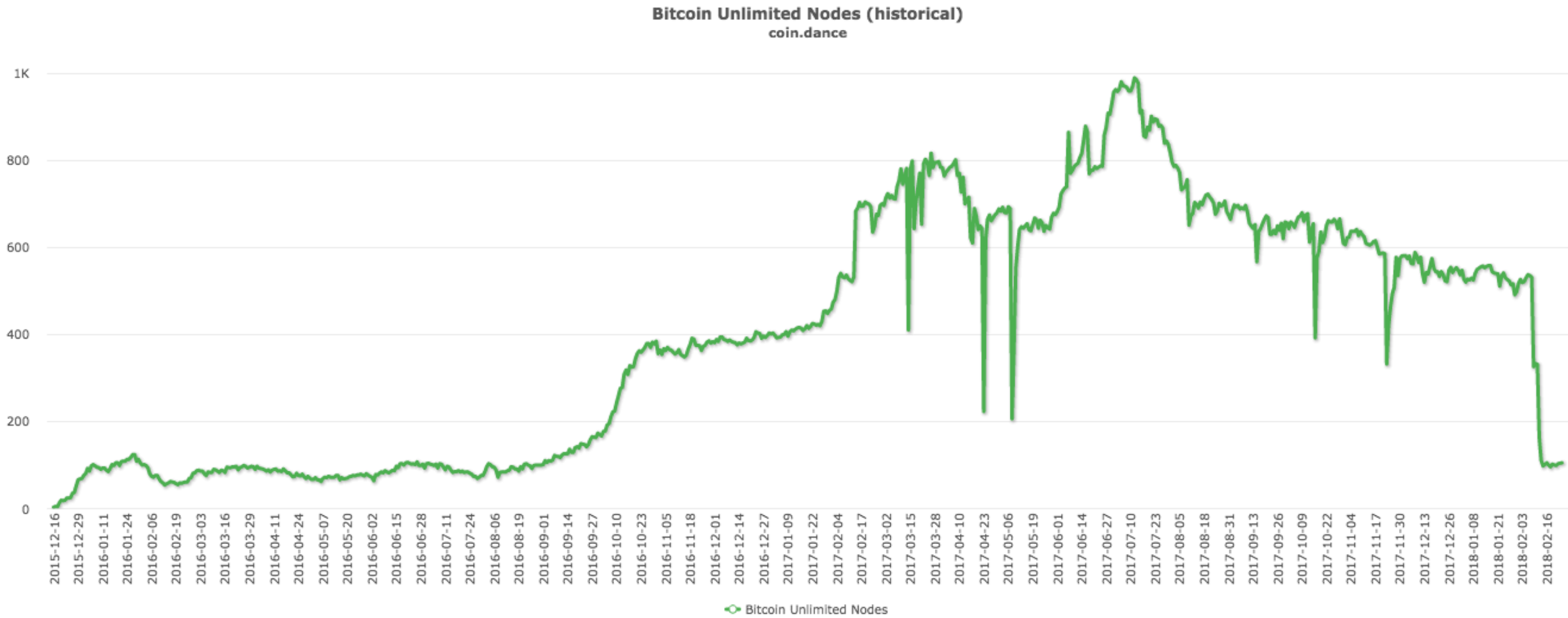
Bitcoin XT is an implementation of a Bitcoin full node that embraces Bitcoin's original vision of simple, reliable, low-cost transactions for everyone in the world. Bitcoin XT originated as a series of patches on top of Bitcoin Core and is now a independently maintained software fork. See our notable features.




Bitcoin XT Nodes (historical)
coin.dance
1.1K
880
660
440
220
0
2015-08-08
2015-08-21
2015-09-03
2015-09-16
2015-09-29
2015-10-12
2015-10-25
2015-11-07
2015-11-20
2015-12-03
2015-12-16
2015-12-29
2016-01-11
2016-01-24
2016-02-06
2016-02-19
2016-03-03
2016-03-16
2016-03-29
2016-04-11
2016-04-24
2016-05-07
2016-05-20
2016-06-02
2016-06-15
2016-06-28
2016-07-11
2016-07-24
2016-08-06
2016-08-19
2016-09-01
2016-09-14
2016-09-27
2016-10-10
2016-10-23
2016-11-05
2016-11-18
2016-12-01
2016-12-14
2016-12-27
2017-01-09
2017-01-22
2017-02-04
2017-02-17
2017-03-02
2017-03-15
2017-03-28
2017-04-10
2017-04-23
2017-05-06
2017-05-19
2017-06-01
2017-06-14
2017-06-27
2017-07-10
2017-07-23
2017-08-05
2017-08-18
2017-08-31
2017-09-13
2017-09-26
2017-10-09
2017-10-22
2017-11-04
Bitcoin XT Nodes

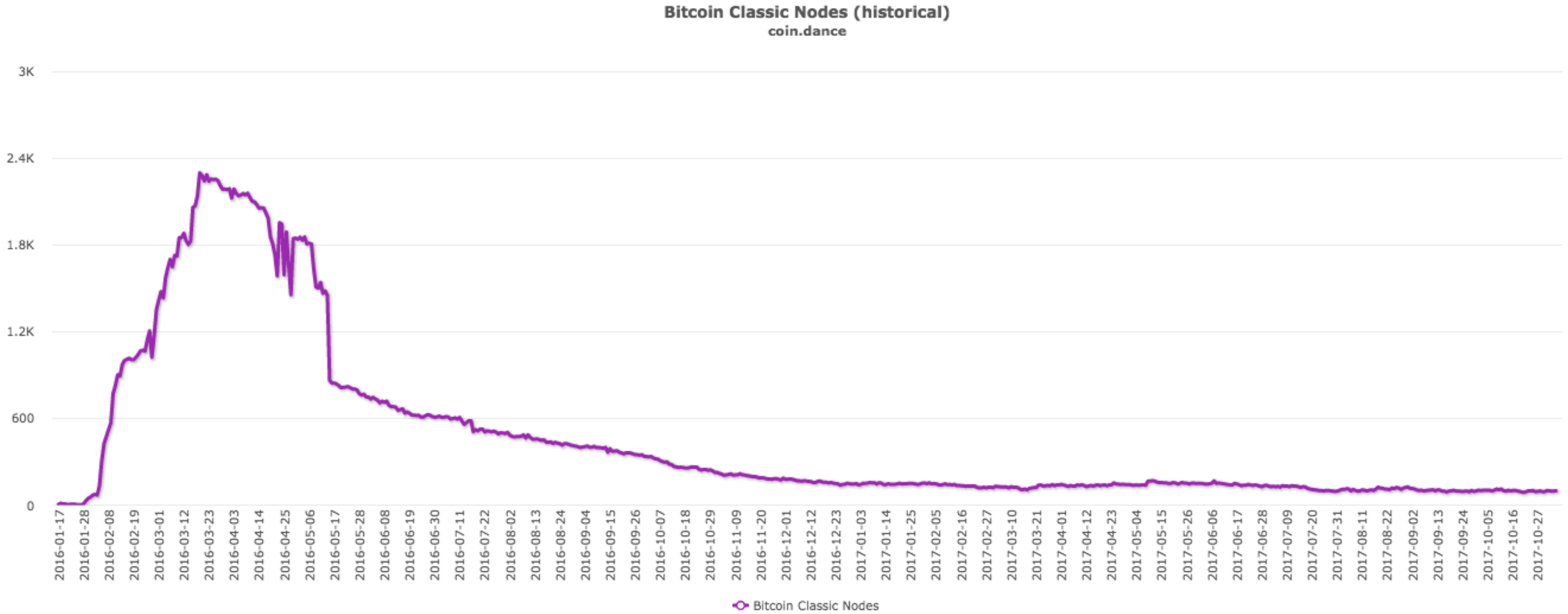
BITCOIN UNLIMITED IMPLEMENTATION

- Created in January 2016 by Peter Rizun and Andrew Stone
- Intention of « providing a voice to all stakeholders in the Bitcoin ecosystem »
- BUIP001 - Fixed block limit made obsolete
- Test 1GB blocks with nChain
- BU node follows the blockchain with most PoW
- Separation of the mining block size (default 1MB) from the non-mining block acceptance size (default 16MB)
- 2% of the Bitcoin nodes , 13% of the Bitcoin Cash nodes


Bitcoin Unlimited Nodes (historical)
coin.dance
1K
800
600
400
200
0
2015-12-16
2015-12-29
2016-01-11
2016-01-24
2016-02-06
2016-02-19
2016-03-03
2016-03-16
2016-03-29
2016-04-11
2016-04-24
2016-05-07
2016-05-20
2016-06-02
2016-06-15
2016-06-28
2016-07-11
2016-07-24
2016-08-06
2016-08-19
2016-09-01
2016-09-14
2016-09-27
2016-10-10
2016-10-23
2016-11-05
2016-11-18
2016-12-01
2016-12-14
2016-12-27
2017-01-09
2017-01-22
2017-02-04
2017-02-17
2017-03-02
2017-03-15
2017-03-28
2017-04-10
2017-04-23
2017-05-06
2017-05-19
2017-06-01
2017-06-14
2017-06-27
2017-07-10
2017-07-23
2017-08-05
2017-08-18
2017-08-31
2017-09-13
2017-09-26
2017-10-09
2017-10-22
2017-11-04
2017-11-17
2017-11-30
2017-12-13
2017-12-26
2018-01-08
2018-01-21
2018-02-03
2018-02-16
Bitcoin Unlimited Nodes

BITCOIN CLASSIC IMPLEMENTATION

- Created in February 2016
- Received support from some Bitcoin companies, developers, investors and miners, such as Coinbase, Bitstamp, Circle, Jeff Garzik, Roger Ver and Gavin Andresen
- Want to increase of the maximum block size from 1Mb to 2 Mb
- November 2016: moved the limit out of the software rules into the hands of the miners and nodes
- November 2017: ceased operation


Bitcoin Classic Nodes (historical)
coin.dance
3K
2.4K
1.8K
1.2K
600
0
2016-01-17
2016-01-28
2016-02-08
2016-02-19
2016-03-01
2016-03-12
2016-03-23
2016-04-03
2016-04-14
2016-04-25
2016-05-06
2016-05-17
2016-05-28
2016-06-08
2016-06-19
2016-06-30
2016-07-11
2016-07-22
2016-08-02
2016-08-13
2016-08-24
2016-09-04
2016-09-15
2016-09-26
2016-10-07
2016-10-18
2016-10-29
2016-11-09
2016-11-20
2016-12-01
2016-12-12
2016-12-23
2017-01-03
2017-01-14
2017-01-25
2017-02-05
2017-02-16
2017-02-27
2017-03-10
2017-03-21
2017-04-01
2017-04-12
2017-04-23
2017-05-04
2017-05-15
2017-05-26
2017-06-06
2017-06-17
2017-06-28
2017-07-09
2017-07-20
2017-07-31
2017-08-11
2017-08-22
2017-09-02
2017-09-13
2017-09-24
2017-10-05
2017-10-16
2017-10-27
Bitcoin Classic Nodes

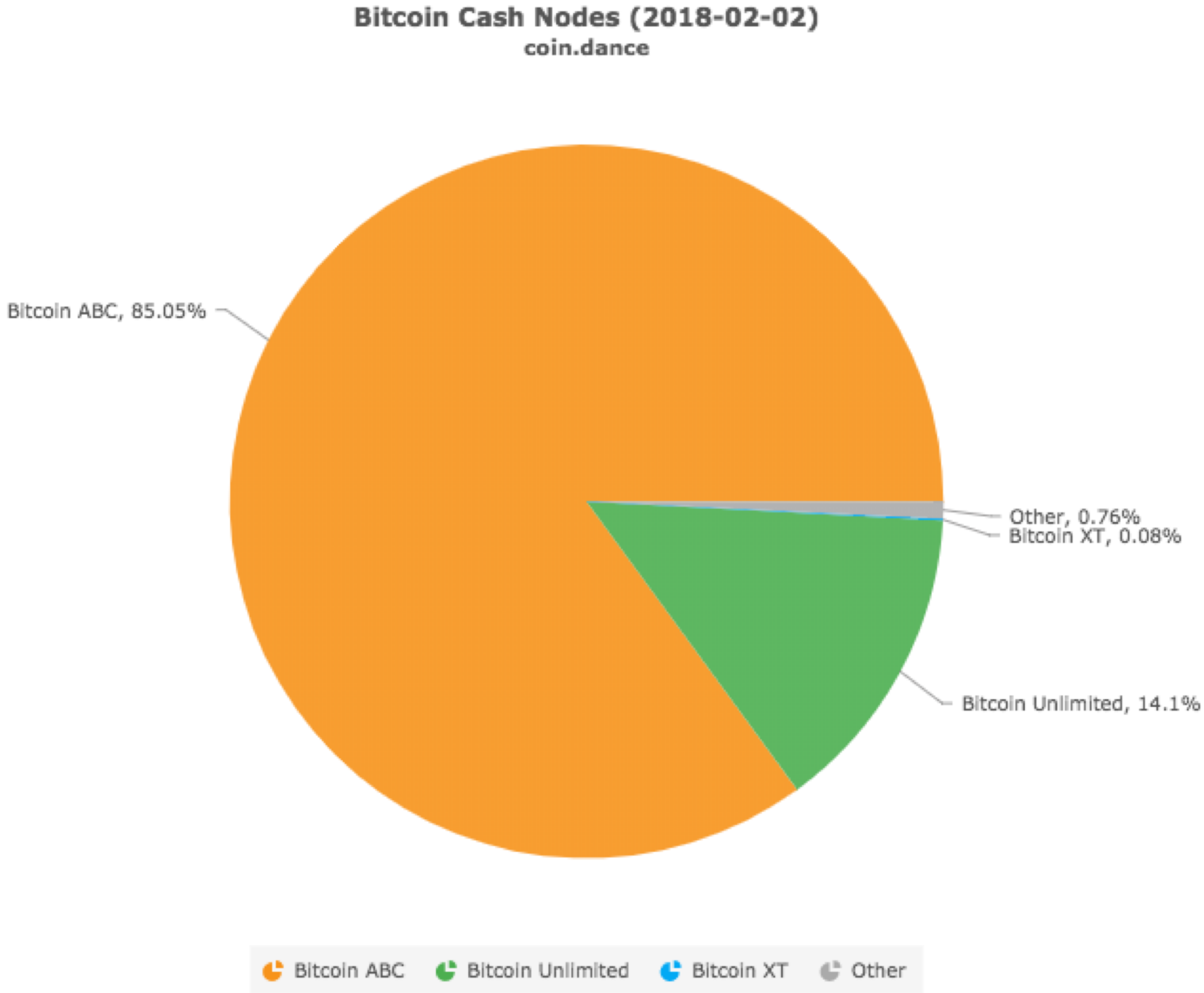
BITCOIN CASH PROTOCOL

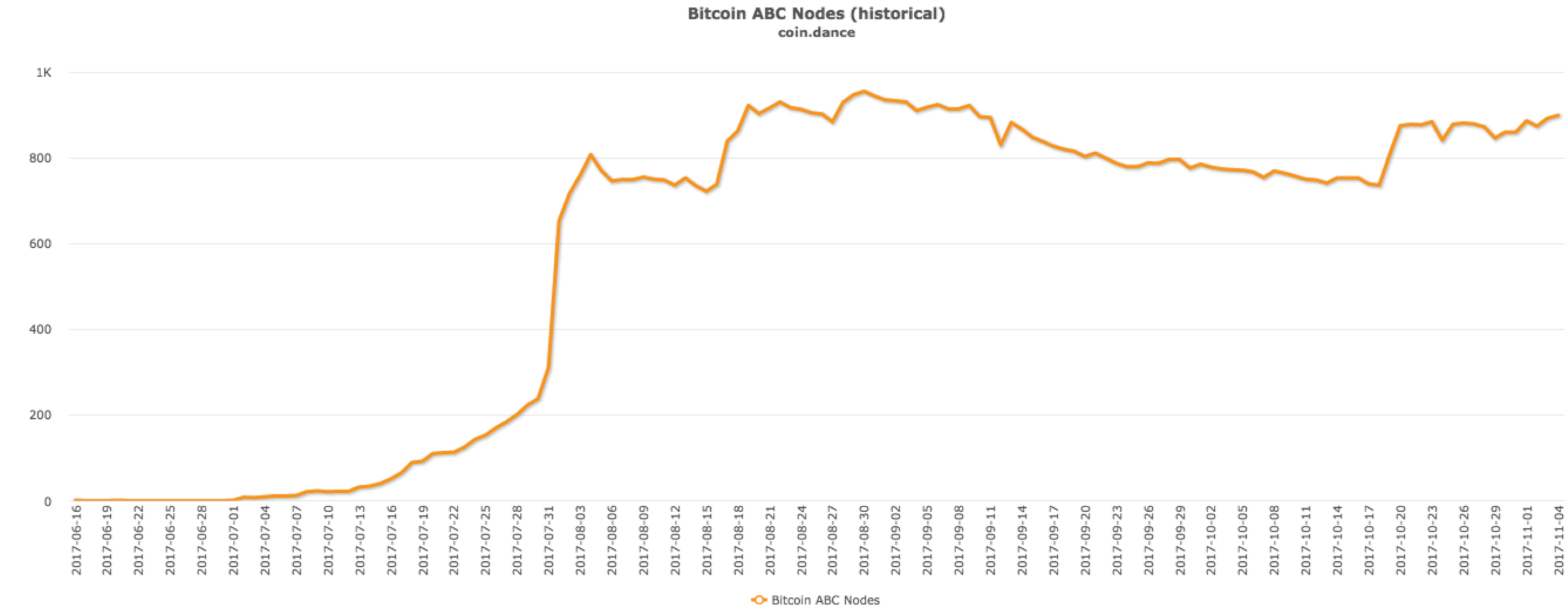
- Hard fork on August 1, 2017

- *Bitcoin ABC:* main implementation of the Bitcoin Cash protocol

- First announced by Bitmain in response to BIP-148 UASF
- Subsequently, some developers took interest in the project (A. Séchet)

- Adjustable Blocksize Cap (in theory)
  - Defaults to 8MB
  - Can be raised up to 32MB


Bitcoin Cash Nodes (2018-02-02)
coin.dance
Bitcoin ABC, 85.05%
Other, 0.76%
Bitcoin XT, 0.08%
Bitcoin Unlimited, 14.1%
Bitcoin ABC
Bitcoin Unlimited
Bitcoin XT
Other


Bitcoin ABC Nodes (historical)
coin.dance
1K
800
600
400
200
0
2017-06-16
2017-06-19
2017-06-22
2017-06-25
2017-06-28
2017-07-01
2017-07-04
2017-07-07
2017-07-10
2017-07-13
2017-07-16
2017-07-19
2017-07-22
2017-07-25
2017-07-28
2017-07-31
2017-08-03
2017-08-06
2017-08-09
2017-08-12
2017-08-15
2017-08-18
2017-08-21
2017-08-24
2017-08-27
2017-08-30
2017-09-02
2017-09-05
2017-09-08
2017-09-11
2017-09-14
2017-09-17
2017-09-20
2017-09-23
2017-09-26
2017-09-29
2017-10-02
2017-10-05
2017-10-08
2017-10-11
2017-10-14
2017-10-17
2017-10-20
2017-10-23
2017-10-26
2017-10-29
2017-11-01
2017-11-04
Bitcoin ABC Nodes

POST-BCASH SCAM FORKS

Name	Current Price	Block Number / Date	Markets?	Official Website	Walleting.Services Extractable?	Market Cap	Circulating Supply	Volume (24h)	% 7d
Bitcoin Cash (BCH)	$1318.34	478558 / Aug 01 2017	High Volume	www.bitcoincash.org	Yes	$22,384,984,740	16,979,675	$689,593,000	-0.16%
Bitcoin Gold (BTG)	$126.68	491407 / Oct 24 2017	High Volume	www.bitcoingold.org	Yes	$2,133,049,906	16,838,361	$41,944,600	0.45%
Bitcore (BTX)	$22.37	492820 / Nov 2 2017	Low Volume	https://bitcore.cc		$258,513,966	11,558,294	$1,710,580	-15.65%
Bitcoin Diamond (BCD)	$17.6932	495866 / Nov 24 2017	Low Volume	http://www.btcd.io	Yes	$?	?	$7,171,730	-32.36%
Bitcoin Lightning (BLG)		498553 / Dec 10 2017		Bitcointalk.org ANN					
Bitcoin Hot (BTH)		498848 / Dec 12 2017		www.bithot.org					
United Bitcoin (UBTC)	$73.7191	498777 / Dec 12 2017	Low Volume	www.ub.com	Yes	$?	?	$918,201	-18.48%
Super Bitcoin (SBTC)	$21.0904	498888 / Dec 14 2017	Low Volume	www.supersmartbitcoin.com	Yes	$?	?	$939,227	-15.45%
BitcoinX (BCX)	$0.00887248	498888 / Dec 14 2017	Low Volume	www.bcx.org	Yes	$?	?	$1,031,790	-12.8%
Oil Bitcoin (OBTC)		498888 / Dec 14 2017		www.oilbitcoin.io					
Bitcoin Neuro (NRO)		498967		bitcointalk thread					
Bitcoin World (BTW)		499777		www.btw.one	Soon				
Bitcoin Faith		500000		www.bitcoinfaith.org	Soon				
Bitcoin God (GOD)	$43.8278	501225 / Dec 25 2017		www.bitcoingod.org		$?	?	$15,243	-3.24%
Bitcoin Atom (BCA)	$24.0734	505888 / Jan 25 / 26		www.bitcoinatom.io		$?	?	$6,571	-24.31%
Bitcoin Uranium (BUM)		Dec 31 2017		www.bitcointalk.org/BUMthread					
Bitcoin Cash Plus		501407		www.bitcoincashplus.org					
Segwit2x (B2X)	$6.23197	501451 / Dec 28 2017	Low Volume	Article	Yes	$?	?	$135,943	-0.45%
Bitcoin Pizza (BPA)		501888		www.p.top					
Bitcoin Smart (BCS)		505050		www.bcs.info					
Bitcoin Interest (BCI)		505083		www.bitcoininterest.io					
Bitcoin Private		Jan / Feb		Reddit					
Bitcoin Lite (BTCL)		Jan / Feb		www.bitcoinlite.us					
Bitcoin Rhodium (BTR)		Airdrops (see website)		www.bitcoinrh.org					
Bytether		478558 / Aug 01 2017		www.bytether.com					
Bitcoin Silver		Scam							
Bitcoin Platnium		Scam							

CONCLUSION

- Blockchain protocol upgrade is not trivial
  - Requires coordination to not lose nodes, or the least possible
  - Not reversible (without damage)
  - Script versioning allows much more flexibility

- The Core team gained experience over the years to deploy hard forks
  - Carefully exploring different upgrade methodologies
  - HFs post-BCH can teach us a lot

- Decentralized governance manifests itself in consensus forks and software implementation choice

- Does size really matter?
  - The whole scaling debate can be seen as a huge waste of time
  - But necessary
  - More urgent issues (privacy)

- Next contentious topics?
  - Energy consumption
  - Privacy

- Bitcoin dramas come and go...

- /r/bitcoin is a BTC subreddit
- /r/btc is a BCH subreddit
- @bitcoin is a BCH twitter
- @btc is a BTC twitter
- http://bitcoin.com is a BCH site
- http://bitcoin.org is a BTC site
- Bitcoin Core is a BTC implementation
- Bitcoin ABC is a BCH implementation

Thank you!