BitMEX Research

A Complete History of Bitcoin's Consensus Forks

28 December 2017

(Source: gryb25)

Abstract

In this piece, we list 19 Bitcoin consensus rule changes (or 18 as an accidental one "failed"), which represents what we believe to be almost every significant such event in Bitcoin's history. At least three of these incidents resulted in an identifiable chainsplit, lasting approximately 51, 24, and six blocks, in 2010, 2013 and 2015, respectively.

BitMEX Research

Filtering out the hype with unbiased, evidence-based reports on the crypto-coin ecosystem.

BitMEX Research is also active on Twitter and Reddit.

research.bitmex.com

Previous reports:

Bitcoin Gold: Investment Flow Data
(21/12/17)

Public Companies with Exposure to the Crypto Space
(13/12/17)

Update: Bitcoin Cash Investment Flow Data
(01/12/17)

Bitcoin's Unique Value Proposition
(29/11/17)

Terminology

Term	Definition
Chainsplit	A split in the blockchain, resulting in two separate chains, with a common ancestor. This can be caused by either a hardfork, a softfork, or neither.
Consensus rule changes	
Hardfork	A loosening of the consensus rules on block validity, such that some blocks previously considered as invalid are now considered valid. Existing nodes are required to upgrade to follow the new hardforked chain.
Softfork	A tightening of the consensus rules on block validity, such that some blocks previously considered as valid are now considered invalid. Existing nodes do not necessarily need to upgrade to follow the new softforked chain.

Note: These terms are believed to have originated in April 2012 and formalized in BIP99 and BIP123.

List of Bitcoin consensus forks

Date	Activation Block Number	Software Version	Description	Type	Outcome
28 July 2010	n/a[1]	0.3.5	OP_RETURN disabled, fixing a critical bug which enabled anyone to spend any Bitcoin.	Softfork	No evidence of any issues during this upgrade.
31 July 2010	n/a[1]	0.3.6	OP_VER and OP_VERIF disabled.[3]	Softfork	Some users had trouble upgrading and it was recommended that nodes should be shut down if they could not be upgraded.[2]
			The addition of the OP_NOP functions, although perhaps there was no usage of OP_NOP prior to this point.	Hardfork	
1 Aug 2010	n/a[1]	0.3.7	Separation of the evaluation of the scriptSig and scriptPubKey. Fixing a critical bug which enabled anyone to spend any Bitcoin	Possibly a non-deterministic hardfork	No evidence of any issues during this upgrade
15 Aug 2010	74,638	0.3.10	Output-value-overflow bug fix following a 184.5-billion Bitcoin spend incident. The 0.5 BTC that was the input to the transaction remains unspent to this day.	Softfork	A chainsplit occurred. Around five hours after the incident, a fix was released, client 0.3.10. It is believed that 51 blocks were generated on the "bad chain" before the "good" chain retook the PoW lead.
			Disabling OP_CAT, which removed a DoS vector, along with the disabling of 14 other functions.	Softfork	
7 Sept 2010	n/a[1]	0.3.12	Adding the 20,000-signature operation limit in an incorrect way. This incorrect limit still exists.	Softfork	No evidence of any issues during this upgrade.

12 Sept 2010	79,400	n/a	Adding the 1MB blocksize limit. The "MAX_BLOCK_SIZE = 1000000" commit occurred on 15 July 2010, which was released in the 0.3.1 rc1 version of the software on 19 July 2010. The commit enforcing the 1MB rule occurred on 7 September 2010, activating at block 79,400. On 20 September 2010, Satoshi removed this activation logic, but kept the 1MB limit.	Softfork	No evidence of any issues during this upgrade.
15 March 2012	171,193	BIP30	Disallow transactions with the same TXID, unless the older one was fully spent. In September 2012, the rule was applied to all blocks, apart from 91,842 and 91,880, which violate the rule.	Softfork	This was a flag-day softfork. There is no evidence of any issues.
1 April 2012	173,805	BIP16	Pay-to-script hash (P2SH) allows transactions to be sent to a script hash (address starting with 3) instead of a public-key hash (addresses starting with 1).	Softfork	55% activation threshold, over blocks in the seven days prior to 1 February 2012. Miners did not upgrade fast enough, so the evaluation point was delayed until 15 March. Users running 0.6.0 rc1 who did not upgrade for the delay activated the softfork early and got stuck on block 170,060 when an invalid transaction, according to their nodes, was mined. After activation, problems were caused as the remaining 45% of miners produced invalid blocks for several months after the softfork.

24 Mar 2013	227,835	BIP34	Requires the coinbase transaction to include the block height.	Softfork	95% activation threshold. A successful rollout occurred.
11 Mar 2013	225,430	0.8.0	This was an unplanned hardfork caused by the migration from Berkeley DB to LevelDB, which accidentally removed an unknown 10,000-BDB database lock limit. This caused a chainsplit on 11 March 2013, although the software which caused the error was released 20 days earlier on 20 February 2013. The change was reverted as the Bitcoin economy and miners switched back to 0.7.2 rules.	No change in the consensus rules	A chainsplit of at least 24 blocks occurred, with the 0.8.0 chain having a maximum lead of 13 blocks. A successful double spend also occurred. The original rules chain eventually re-took the PoW lead.
18 Mar 2013	n/a[1]	0.8.1	This was a temporary softfork, introducing a new rule requiring that no more than 4,500 TXIDs are referenced by inputs in a block. This rule is stricter than the 10,000-BDB lock limit. The rule expired on 15 May 2013, a flag-day hardfork.	Softfork	There is no evidence of any issues.
15 May 2013 or 16 Aug 2013	252,451 or earlier	BIP50	In August 2013, a block may have been produced that violated the original 10,000-BDB lock limit rule, which was relaxed on 15 May 2013.	Hardfork	There is no evidence of any issues.
4 July 2015	363,731	BIP66	Strict DER signature upgrade means Bitcoin is no longer dependent on OpenSSL's signature parsing.	Softfork	95% threshold over a 1,000-block period. A chainsplit occurred, lasting six blocks, as some miners signaled support for BIP66 but had not upgraded and were SPY mining. The new softfork rules chain eventually took the lead.

14 Dec 2015	388,380	BIP65	Check Lock Time Verify enables funds to be locked until a specific time in the future. This is Bitcoin's first new function.	Softfork	Successful rollout using a 95% threshold.
4 July 2016	419,328	BIP68 BIP112 BIP113	Relative lock-time enables a transaction output to be banned for a relative amount of time after the transaction. CheckSequenceVerify. Median time-past removes the incentive for a miner to use a future block timestamp to grab more transaction fees.	Softfork	Successful rollout using 95% versionbits signaling.
23 July 2017	477,800	BIP91	This temporary softfork makes signaling for the SegWit upgrade mandatory.	Softfork	Softfork successfully activated with an 80% miner threshold over a 336-block period, although only a tiny minority of users enforced BIP91 rules, which have since expired. Therefore, the risk of a chainsplit was elevated in this period.
01 Aug 2017	478,479	BIP148	This temporary softfork makes signaling for the SegWit upgrade mandatory for a two week period following 1 August 2017.	Softfork	Flag-day softfork appeared to succeed with no issues, although only a minority of users enforced BIP148 rules, which have since expired. Therefore, the risk of a chainsplit was elevated in this period.
24 Aug 2017	481,824	BIP141 BIP143 BIP147	The segregated-witness (SegWit) upgrade.	Softfork	Rollout using 95% versionbits signaling.

The year 2262	13,440,000	BIP42	Fixed a 21 million coin supply cap bug. The software was upgraded in April 2014 to fix this bug, but the new rule does not apply until the 23rd century.	Softfork	The softfork is not applicable yet.

(**Source:** BitMEX Research, Github, Bitcoin blockchain)

Notes

1. With the exception of the 1MB blocksize limit, prior to the 2012 BIP16 softfork, there was no activation methodology, so if the fork occurred smoothly without a chainsplit, there is not necessarily a specific block height or date on which the consensus fork occurred.
2. "If you can't upgrade to 0.3.6 right away, it's best to shut down your Bitcoin node until you do." — Satoshi Nakamoto
3. Prior to the removal of OP_VER, each software upgrade could potentially be considered a non-deterministic hardfork and these have been excluded from this list. If the definition of hardforks does include this, then it's a somewhat pedantic definition.
4. There are no consistent definitions used in the above table because, for example, a different definition of the date on which the fork occurred may be more relevant in each incident, depending on the circumstances.
5. Others have mentioned that changes to the P2P protocol can also be considered hardforks if they make previous software releases unusable, since they can no longer connect to the network. Strictly speaking, however, these do not relax the rules on block validity and one could sync old nodes by setting up a relay of intermediary versions of the software. These changes are excluded from the above list.
6. Some consider BIP90 a hardfork, but since it only relaxed rules related to softfork activations that happened in the past, it does not share many of the characteristics or risks normally associated with consensus forks. Using the same logic, the block checkpoint scheme can also be considered as softforks.
7. In July 2010, the chain selection rule was altered to shift to most accumulated work from the number of blocks. Technically, this is not a change to block validity rules; however, this change does share some of the risks associated with consensus rule changes.
8. After the publication of this piece, an alternative list of consensus versions was published on the Bitcoin Wiki.

Was the 2013 incident a hardfork?

In our view, on balance, the increase in the BDB lock limit a few months after the 11 March 2013 chainsplit was a hardfork. The rule in question was a 10,000-BDB lock limit, which was increased. The rule was relaxed on 15 May 2013 in software version 0.8.1, which was released on 18 March 2013. A block exceeding this limit may finally have been produced on 16 August 2013 so one can define the date of the hardfork to be either 15 May 2013 or 16 August 2013.

Some have argued that this may not have been a hardfork for a variety of reasons, including that this rule was "quasi-non-deterministic" or that one could manually change the BDB config settings. Indeed, due to the non-deterministic nature of the lock limit, perhaps it is theoretically possible one could have a local system set up such that the old BDB lock limit has never been breached. Therefore, one could declare that there has "never been a hardfork" in Bitcoin, following a strict definition that requires a hardfork to be deterministic or perhaps even directly related to Bitcoin data such as transactions or the block header.

When discussing this incident, Bitcoin developer Gregory Maxwell said:

> *"Sort of a mixed bag there, you can actually take a pre BIP-50 node and fully sync the blockchain, I last did this with 0.3.24 a few months ago. It just will not reliably handle reorgs involving large blocks unless you change the BDB config too. So it's debatable if this is a hard fork either, since it's quasi-non-deterministic. There were prior bugs fixed where older versions would get stuck and stop syncing the chain before that too... So I think by a really strong definition of creating a blockchain which violates the rules mandated by prior versions we have never had a hardfork."*

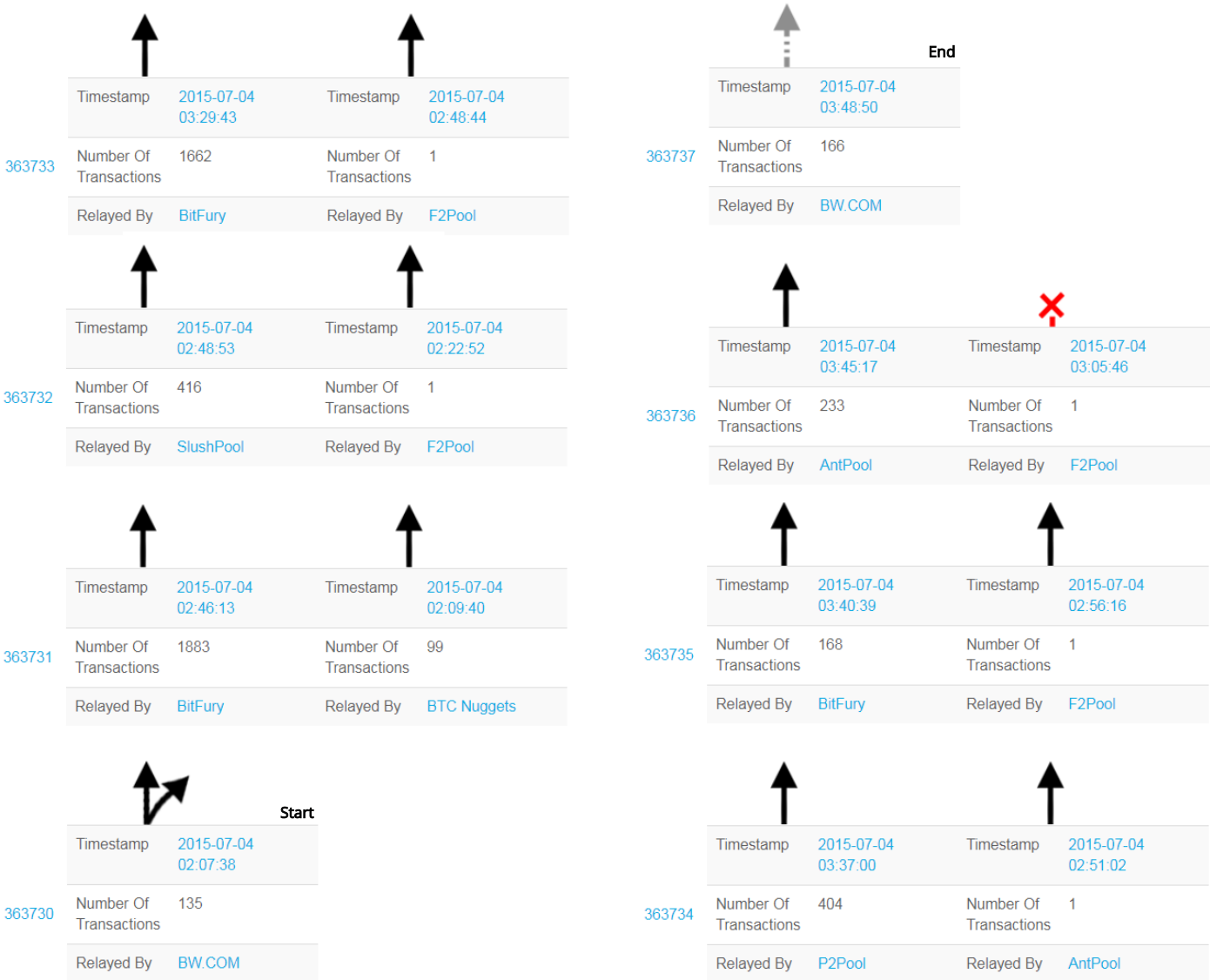
Chainsplit incident of July 2015

In the list of consensus rules changes above, there are three incidents that caused identifiable chainsplits. The most recent of these occurred on 4 July 2015, during the BIP66 softfork upgrade.

Immediately after the activation of BIP66, there was a six-block orphan chain created because a miner produced an invalid block that was not recognised as invalid by some other mining pools, because they were not validating new blocks.

In this case, some miners signalled support for the BIP66 softfork but hadn't actually upgraded their nodes to validate; one could say miners were "false flagging". If the miners had been validating blocks, they would have discovered the block was invalid and rejected it. Instead, some miners built on top of the invalid block and a chainsplit occurred.

A diagram illustrating these six blocks and the chainfork is displayed below.



Graphical illustration of the July 2015 chainsplit.
(Source: Blockchain.info, http://archive.is/WqGRp and http://archive.is/LHlF7**)**

Disclaimer

Transacting on BitMEX is not offered or available to any resident of (I) the United States of America, (ii) Cuba, Crimea and Sevastopol, Iran, Syria, North Korea, Sudan, or any other sanctioned jurisdiction, or (iii) any jurisdiction where the services offered by BitMEX are restricted.

This material should not be the basis for making investment decisions, nor be construed as a recommendation to engage in investment transactions and is not related to the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting or any other related services, nor is a recommendation being provided to buy, sell or purchase any good or product.

Any views expressed are the personal views of the authors of the report. BitMEX (or any affiliated entity) has not been involved in producing this report and the views contained in this report may differ from the views or opinions of BitMEX.

The information and data herein have been obtained from sources we believe to be reliable. Such information has not been verified and we make no representation or warranty as to its accuracy, completeness or correctness. Any opinions or estimates herein reflect the judgment of the authors of the report at the date of this communication and are subject to change at any time without notice. BitMEX will not be liable whatsoever for any direct or consequential loss arising from the use of this publication/communication or its contents.