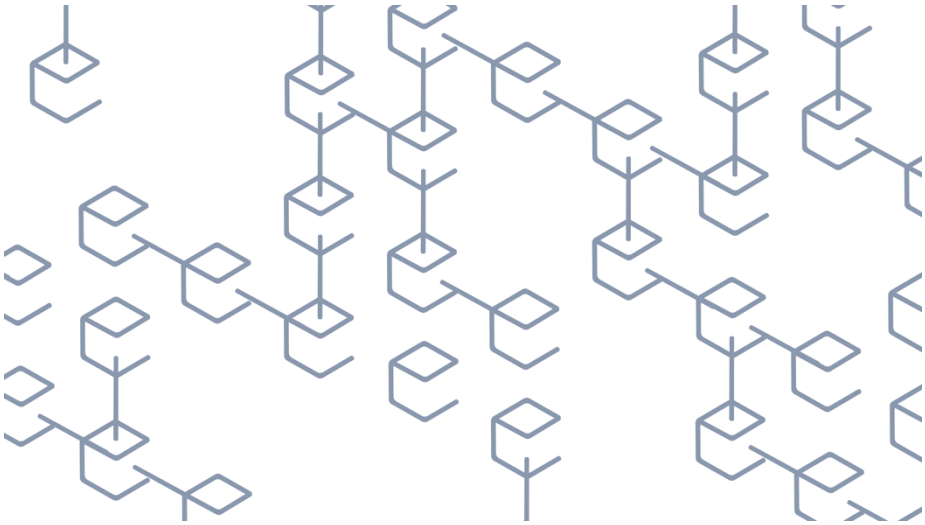
BitMEX Research

Diagram of a Bitcoin Block: Covert versus Overt AsicBoost

01 March 2018



(Source: UCC)

Abstract

We present a graphical illustration of a Bitcoin block, including the Merkle trees and explain why the additional Merkle tree in the block, associated with the Segregated Witness upgrade, is necessary. We then take a closer look at some of the potential negatives of both overt and covert AsicBoost, following on from our September 2017 piece on the subject. After the recent announcement from the patent owner, we conclude that the new Blockchain Defensive Patent License (BDPL) scheme, if robust, could result in limited downsides to the use of overt AsicBoost on the network. On the other hand, there may still be some issues with the less efficient covert AsicBoost.

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:

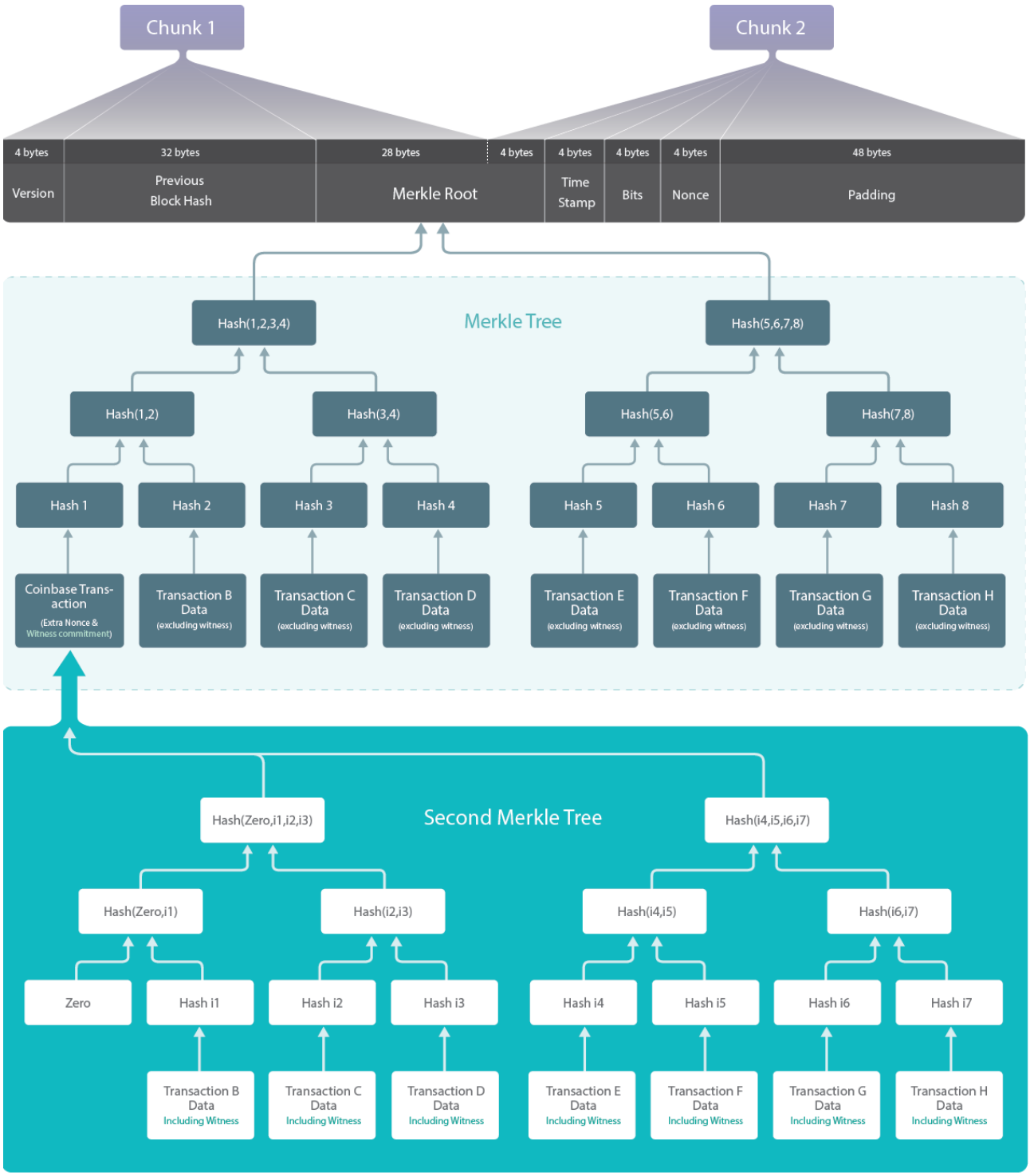
Tether
(18/02/18)

A Blockchain-Specific Defensive Patent Licence
(14/02/18)

The Ripple Story
(06/02/18)

The Art of Making Softforks: Protection by Policy Rule
(01/02/18)

The Lightning Network
(25/01/18)



This is a simplified depiction of the structure of a Bitcoin block and the Merkle trees inside it. Other, more detailed illustrations have been produced by Jeremy Rubin and Timo Hanke.
(Source: BitMEX Research**)**

Components of the diagram

Block header

The header of the Bitcoin block (in grey) is around 80 bytes and includes the version, the hash of the previous block, the Merkle root, the timestamp, the bits (difficulty), and the nonce.

Block header candidate

This includes all of the above, with the exception of the nonce.

Chunks

The diagram above shows that the Merkle root is split between two chunks, which are required to conduct Bitcoin's SHA256 proof-of-work function. An explanation of this can be found in our earlier piece on AsicBoost.

Second Merkle tree

The SegWit upgrade introduced a new Merkle tree, which has the same structure as the main Merkle tree, except that it includes the witness data and excludes the coinbase transaction. The relative position of each transaction must remain identical to that of the main Merkle tree.

Why a second Merkle tree?

The second Merkle tree increases complexity, which some may consider a disadvantage. SegWit was an upgrade to the Bitcoin network that fixed bugs, such as the quadratic scaling of sighash operations and transaction malleability. The witness data could not be added into the main Merkle tree, as otherwise old nodes would consider these transactions invalid, which would be a hardfork.

However, it is not true to say the additional Merkle tree could be avoided by making SegWit a hardfork upgrade rather than a softfork upgrade. A hardfork resulting from the inclusion of witness data in the main Merkle tree would lead existing wallets to consider the new transaction format invalid, and these wallets would not be compatible with the new transaction format whether they were fully verifying nodes or not. The effect of this would be that some users would be unable to interact with each other and funds could appear to go missing. This type of upgrade may not be possible in a live network such as Bitcoin without significant disruption. Therefore, the additional complexity of a second Merkle tree would be necessary even if the SegWit upgrade were a hardfork.

AsicBoost

As we explained in our previous piece on AsicBoost, covert AsicBoost involves finding a collision in the last 4 bytes of the Merkle root, exploiting the fact that the

hashing algorithm splits the Merkle root between the two chunks. Covert AsicBoost messes with the transactions, something that overt AsicBoost avoids. The second Merkle tree can make covert AsicBoost more difficult unless the blocks are much smaller, which could be detectable.

Potential negative issues with AsicBoost

	Covert AsicBoost	Overt AsicBoost
Patent protection	This potential negative of AsicBoost applies to both the covert and overt type. AsicBoost is a patented technology and, as we explained in our previous piece on patents, these can be particularly damaging in the blockchain space. This appears to be one of the primary negatives of AsicBoost, as it could potentially give one mining company an insurmountable advantage over the competition, resulting in a gap that could not be closed due to legal restrictions. This could undermine Bitcoin's core value proposition. It is possible that the Bitcoin community would conduct a softfork to block AsicBoost if the patent problem becomes significant. To mitigate this problem, the patent owner could open the patent — for example, by making a defensive patent pledge. It appears as if the AsicBoost patent owner may have recently made such a pledge. If the pledge proves robust enough, this issue may now be resolved, at least in the regions the patent applies.	
Smaller blocks and lower capacity	Covert AsicBoost can incentivise the production of smaller or even empty blocks, which makes covert AsicBoost more efficient. This can then reduce the capacity of the network and increase transaction fees. Smaller or empty blocks have a negative impact on capacity, since they still maintain the network difficulty but do not make a significant contribution to any transaction backlog.	n/a
Unwillingness to upgrade to SegWit and potential dishonesty over the reason	Perhaps the most damaging negative of AsicBoost was that it may have caused some miners to be unwilling to upgrade to SegWit. This in itself may not be much of a negative, but the supposed dishonest and divisive misinformation campaign about SegWit may have had a large negative impact on the ecosystem. However we would like to point out that this is merely an uncertain, unsubstantiated accusation, and it is not clear if this was a motivating factor behind opposition to SegWit.	n/a

Incentive to adjust the Merkle trees or transactions	As the diagram above illustrates, covert AsicBoost relies on the ability of the miner to adjust the Merkle tree or the transactions. This could have detrimental effects on the network other than smaller blocks. Overt AsicBoost appears to be a much cleaner solution, needing only a field in the block header to be changed.	n/a
Secret advantage over competition	Covert AsicBoost may be undetectable and therefore may provide some miners a secret advantage over the competition, compared to a known advantage. Although in general we think transparency is a good thing, it's not clear whether or not the network on which covert AsicBoost operates suffers any direct disadvantage from the secrecy, apart from what is mentioned elsewhere in this table.	n/a
Reduced ability to conduct softfork upgrades via version signalling and a warning message in Bitcoin Core	n/a	Overt AsicBoost uses the version field, seen on the top left of the illustration above. This has been used as a signal, to indicate that a miner is ready to upgrade via a softfork. Overt AsicBoost may use space in this field, which may prevent its use as an upgrade-signalling system. However: 1. Overt AsicBoost may not require all 4 bytes and therefore some bytes may be left for softfork signalling. This could reduce the number of softforks that can occur simultaneously. 2. Many regard the softfork signalling system to have been a failure anyway. Miners often provide simultaneous contradictory signals, rendering the signal methodology unreliable. Another downside of overt AsicBoost is that Bitcoin Core software may see an unusual version field and think the network is upgrading in an unknown manner, resulting in a warning message to the user.

In our view, AsicBoost is not necessarily a negative for the network. Although covert AsicBoost has problems with an incentive to produce smaller blocks, most of the issues related to overt AsicBoost can be mitigated. In particular, if the BDPL system proves robust, there may be no significant negatives resulting from the use of overt AsicBoost — at least none which we can currently predict.

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.