Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Bitcoin Scaling Solutions And Their Downsides

Simona Mola

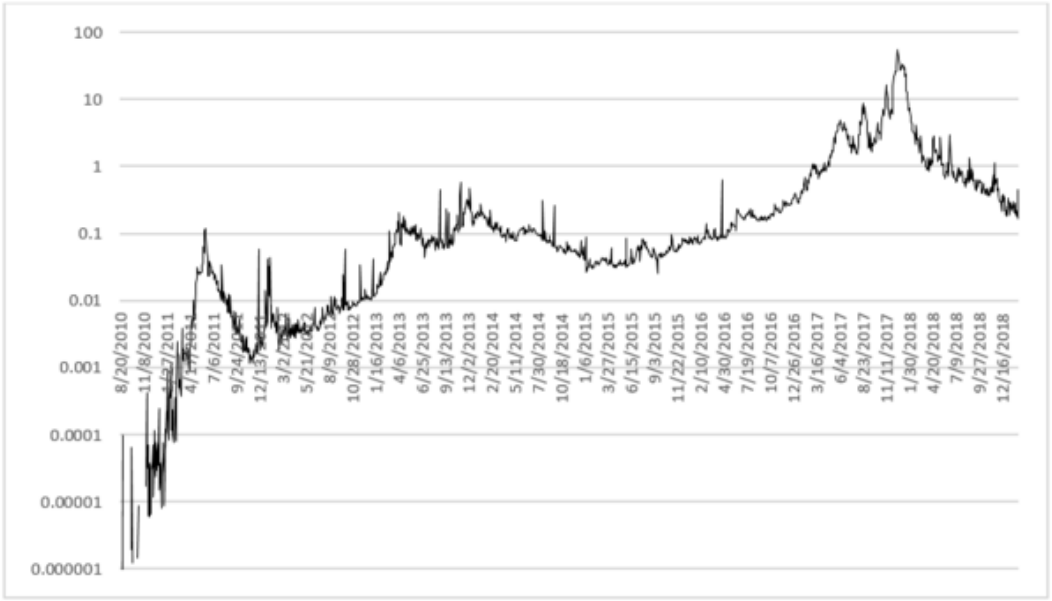
Zhong Zhang

By **Simona Mola and Zhong Zhang** (March 6, 2019, 12:35 PM EST)

Bitcoin was designed as a decentralized monetary system and an alternative to central banking. Decentralization implies that no one can unilaterally change the way bitcoin works or its transaction history. Since Satoshi Nakamoto released the original bitcoin whitepaper in 2010,[1] reaching and maintaining decentralization has been the priority of all technological developments. To this end, bitcoin relies on its technological design: open source software, public-key cryptography, blockchain data structure, proof-of-work mining and distributed full nodes.

However, it is well known that bitcoin has a scalability problem.[2] We have all heard at least once the comparison between bitcoin and Visa in terms of transaction capacity. That is, while Visa handles an average of 150 million transactions per day as of the end of 2018,[3] bitcoin network processes about 280,000 transactions per day.[4] This capacity is not enough to serve as a global digital medium of exchange.

Bitcoin Average Transaction Fee in USD



Besides the comparison with Visa, which may not be quite parallel, bitcoin's scaling problem is reflected in its average transaction fees. In the situation of greater market demand for bitcoin transactions, the restriction of the block size to 1 MB leads to a higher average wait time before confirmation and thus greater transaction fees. As showed in the image above, for example, when market demand for bitcoin transactions spiked in late 2017, it cost about $50 on average to complete one transaction.[5] Although bitcoin's transaction fee has since lowered to about $0.20 per transaction, the scalability issue bitcoin faced has been widely recognized and discussed.

Bitcoin creates, on average, one block per 10 minutes, so the 1 MB block size limit implies that bitcoin can only process about 52.6 GB of transaction data annually at full capacity. This annual transaction limit of 52.6 GB is a hard constraint of bitcoin's market for transaction confirmation, where the cost of sending bitcoin is determined by market forces.

First, the data size of each bitcoin transaction depends on its complexity, not on its value. That is, it takes more data to send one bitcoin to five different addresses than to send five bitcoins to one address. Second, bitcoin users can include an optional transaction fee to "tip" those miners who select and process transactions into a new block. For-profit miners typically select the validated transactions with the highest total "tips" as their input for mining the next block, subject to the 1 MB block size limit.[6]

Current Solutions

Multiple projects are currently in development that address bitcoin's scaling problem. We can categorize them as on-chain solutions versus off-chain solutions. On-chain means that the project will amend bitcoin's current code base, changing its functions to enable scalability. Off-chain means that the project will not touch bitcoin's code base, but instead seek institutional solutions.

Some on-chain solutions require significant changes to bitcoin's fundamental parameters on its base layer; others leave the base-layer settings unaltered but develop second-layer "derivatives" to scale bitcoin. A close analogy is as follows: the internet is the base layer, while applications (like emails) based on the internet are its second-layer "derivatives."

Base-Layer On-Chain Solutions: Increasing Block Size

The most straightforward way to increase bitcoin's transaction capacity is to increase its block size.[7]

The clearest benefit of a larger block size is that it is ready to implement. Bitcoin full node operators simply need to update their software to a version with increased block size parameters. The professional bitcoin mining industry also welcomes bigger blocks, as it has the resources to easily absorb the additional cost associated with larger blocks.

The disadvantages of scaling bitcoin by increasing block size are, however, prominent. First, increasing block size is not a long-term solution for scaling, as market demand for transactions will soon reach the capacity provided by the increased block size — just like wider roads are not necessarily an effective solution for traffic jams. Second, larger blocks would make it more costly to maintain a complete copy of transaction data and thus a full node, potentially harming the decentralization of the distributed network. Third, larger blocks give professional miners more power in the ecosystem, as they can better absorb the higher maintenance costs. Even if miners themselves are not manipulating bitcoin, large mining facilities are easier targets for external attacks, thus reducing its security.

The issue about bitcoin's block size ultimately led to the "Bitcoin Civil War" of 2017.[8] On Aug. 1, 2017, the majority of bitcoin users activated the user activated soft fork[9] named Segregated Witness, or SegWit. This upgrade was intended to increase bitcoin's block capacity to 4 MB, along with other improvements, without a hard fork.[10] While other bitcoin users who opposed SegWit initiated a hard fork that increased block size to 8 MB, creating a new cryptocurrency called bitcoin cash,[11] the crypto community has ultimately chosen SegWit as the base layer solution for scaling bitcoin. As a matter of fact, as of January 2019, bitcoin cash is only 3.6 percent of bitcoin's market capitalization and total hashrate.

Second-Layer On-Chain Solutions

Scaling through developing second-layer applications is currently the focus of many developers.[12] Lightning Network and Sidechain are the two most developed implementations.

Lightning Network

Lightning Network[13] utilizes a smart contract called Hashed Timelock Contract[14] to establish "payment channels" between bitcoin users. Once a payment channel is established between two users, they no longer have to confirm every single transaction between them on the bitcoin network. Instead, they only have to confirm the open balance with a channel-opening transaction and the ending balance with a channel-closing transaction.

All other transactions between them are handled by adjusting their relative balance without confirmation on the network. Imagine that conducting a base-layer bitcoin transaction is like confirming every single transaction of your monthly credit card statement, while LN only has to confirm your month-begin and month-end credit balances. LN also allows two users who are not directly channel-connected to transact by routing transactions through other users.

There are several advantages of scaling bitcoin with LN. First, LN is based on bitcoin and does not require its own token to operate. Second, as adjusting relative balances within each payment channel can be done instantly, the transaction capacity of LN is theoretically unlimited, putting no extra burden on bitcoin's infrastructure. Third, LN is based on HTLC, which is "trust-free," meaning that the system works without users trusting each other.

There are also several disadvantages of using LN. First, it is still in development and requires technical skills and special equipment to operate. Second, LN requires users to lock up a certain amount of bitcoin to use. For example, if two users want to establish a payment channel that has a certain maximum balance of bitcoins, both of them have to deposit and lock that amount of bitcoins in the HTLC while their channel is open. Third, as routing is required to connect two users without a direct channel connection, an optional routing fee is included in LN's design to give other users incentive to cooperate. If LN does achieve its goals and mass market adoption, then this routing fee may create unforeseen economic challenges, just like the transaction fee on bitcoin's base layer. [15]

Sidechain

A sidechain is a parallel blockchain with relaxed limits in terms of transaction capacity and/or computational functions. A sidechain usually requires its own token, which is pegged to bitcoin on the main chain. For example, if a sidechain with TCcoin as its token allows a Turing-Complete[16] smart contract, a user can convert bitcoins into TCcoins, execute the contract on the sidechain and eventually

convert the final amount of TCcoin back to bitcoin.

The greatest advantage of sidechain is that it provides flexibility in cryptocurrency design without affecting the functionality of bitcoin itself. It is a way to conduct isolated experiments that may have serious outcomes if implemented directly on bitcoin. Sidechain also allows the issue of a bitcoin-based "smart asset" without an initial coin offering.

Sidechain also faces several disadvantages. First, there is not yet a complete trust-free method to enforce the peg between bitcoin and sidechain's token. This means that users of the sidechain have to trust sidechain operators to honor the peg and exchange rate. Second, most sidechain designs require computing power to secure functionality, just like bitcoin requires proof-of-work mining. This means sidechain not only consumes additional energy to operate but also requires a working mechanism to incentivize miners.[17]

Off-Chain Solutions

Off-chain solutions for scaling bitcoin are usually proposed by trusted institutions in traditional capital markets. They offer bitcoin off-chain transaction service based on users' trust in these institutions' reputation, thus requiring no change to bitcoin's technology.

A good example is the proposed Bakkt exchange[18] from Intercontinental Exchange, which owns the New York Stock Exchange and is among the largest exchange operators of the world. As an exchange, Bakkt will hold bitcoin and internalize bitcoin transactions between its customers. Thus, Bakkt only has to make on-chain bitcoin transactions when it has to increase or decrease its total holding. Bakkt can also facilitate bitcoin-based contracts between its customers without using smart contracts on the blockchain.

Obviously, this type of off-chain solution requires trust between parties in the same way the current financial market requires. Although countering bitcoin's original purpose of building a trust-free alternative monetary system, such off-chain solutions may prove to be valuable options for the success of bitcoin as bitcoin continues to mature and traditional institutions continue to adopt.

Legal Implications and Conclusion

In sum, scaling solutions may require compromising the principle of decentralization, with relevant legal implications for all the parties involved in the bitcoin ecosystem.

In this regard, William Hinman, director of the U.S. Securities and Exchange Commission's Division of Corporation Finance, commented that, as there is no "a central third party whose efforts are a key determining factor in the enterprise … [t]he network on which bitcoin functions is operational and appears to have been decentralized for some time, perhaps from inception."[19] He then concluded that, as bitcoin is decentralized, the offer and resale of bitcoin are not subject to securities laws.

The process of scaling bitcoin may create, however, new digital assets that can be subject to securities laws. Given that regulators have not yet clarified the required degree of decentralization, this is a particularly relevant issue. For example, if the scaling process results in a hard fork that creates a new digital asset mainly supported by entities that are organized in a traditional centralized fashion (e.g., holding companies, partnerships, etc.), such new asset could be deemed a security.

Similarly, when scaling bitcoin with a sidechain operated by a centralized entity, the sidechain token that is pegged to bitcoin could be also deemed a security. Therefore, holders of a decentralized cryptocurrency like bitcoin may find themselves holding newly created securities after some technical change in the blockchain.

Furthermore, to the extent that scaling solutions impact decentralization, questions on the security and privacy of the transactions may rise. For example, some have raised concerns about the vulnerability of sidechain technology to the double-spending problem.[20] The issue hinges on the level of trust established by sidechain operators and on the economic incentives in place to ensure penalties for bad behavior. However, even in a trust-free payment channel supported by LN, similar security concerns may rise.

Given that maintaining a payment channel requires locking up an amount of bitcoins equal to the channel capacity for the duration of the channel, lightning nodes with more bitcoins are more capable at connecting and routing payments for a fee. This may incentivize LN operators to consolidate their small nodes into a single centralized large node, with anti-competitive effects.

Finally, because LN payments occur in separate channels, privacy experts have voiced concerns over the ability of a lightning node to pry into the contents of a transaction.[21] This could lead to a rogue node attempting to collect and sell this information to governments or corporations. The privacy concerns could be exacerbated if large centralized nodes route a significant portion of transactions.

As on- and off-chain solutions continue to be developed to address the bitcoin scalability problem, more clarity will unfold on the full range of legal implications involving the parties within the bitcoin ecosystem.

Simona Mola is a manager and Zhong Zhang is a senior economist at Bates White LLC.

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2010, available at https://Bitcoin.org/Bitcoin.pdf.

[2] Bitcoin’s scalability problem relates to the concerns about the limits on the volume of transactions the bitcoin network can process.

[3] Jan Vermeulen, “VisaNet–Handling 100,000 Transactions per Minute,” Dec. 17, 2016, available at https://mybroadband.co.za/news/security/190348-Visanet-handling-100000-transactions-per-minute.html.

[4] See Blockchain, “Confirmed Transactions per Day,” accessed [2/19/2019], https://www.blockchain.com/charts/n-transactions?timespan=all.

[5] Figure 1 data come from https://www.blockchain.com/charts. We calculated average transaction fee from data on total transaction fee and number of transactions. Accessed [2/12/2019].

[6] For example, if one user requires immediate transaction confirmation in the next block, she could include a large tip with her transaction so that it will be picked up by miners immediately. If another user can afford to wait, she could include a small tip or even no tip with her transaction. Then her transaction will be selected by miners only after more profitable transactions have been served first. The market price for bitcoin transaction fees solely depends on the demand for transaction confirmation and the supply of miner service.

[7] Another way is to increase the block mining frequency. However, because of the consideration against Distributed Denial-of-Service (DDoS) Attacks, the bitcoin community generally agrees that block frequency should not be increased, so increasing block size becomes the remaining option. See "Denial of Service Attacks," accessed [2/19/2019], https://en.bitcoin.it/wiki/Weaknesses#Denial_of_Service_.28DoS.29_attacks.

[8] Aziz, "Bitcoin's Civil War: How and Why?" Masterthecrypto, accessed [2/19/2019], https://masterthecrypto.com/bitcoins-civil-war-how-and-why/.

[9] See https://bitcoin.org/en/glossary/uasf

[10] See https://en.wikipedia.org/wiki/Fork_(blockchain)#Hard_fork

[11] See https://en.wikipedia.org/wiki/Bitcoin_Cash

[12] As any change to bitcoin's base layer may have unintended consequences for the cybersecurity and decentralization of bitcoin.

[13] See https://en.wikipedia.org/wiki/Lightning_Network

[14] See Bitcoin Wiki, "Hashed Timelock Contracts," accessed [2/19/2019], https://en.bitcoinwiki.org/wiki/Hashed_Timelock_Contracts

[15] Currently, there are several independent implementations of LN, including a non-commercial project by MIT Digital Currency Initiative (Digital Currency Initiative, "Layer 2: The Lightning Network," accessed [2/19/2019], https://dci.mit.edu/lightning-network/); Blockstream's c-lightning (Blockstream, "Lighting Network," accessed [2/19/2019], https://blockstream.com/lightning/); ACINQ's éclair (ACINQ, "Homepage, "accessed [2/19/2019], https://acinq.co/); and Lightning Labs' Ind (Lightening, "The Lightning Network," accessed [2/19/2019], https://lightning.engineering/technology.html).

[16] See https://en.wikipedia.org/wiki/Turing_completeness

[17] Currently, there are several independent Bitcoin sidechain projects, including Rootstock (RSK, "Homepage," accessed [2/19/2019], https://www.rsk.co/); Blockstream's Liquid (Blockstream, "Liquid," accessed [2/19/2019], https://blockstream.com/liquid/); and Drivechain (Drivechain, "Homepage," accessed [2/19/2019], http://www.drivechain.info/).

[18] See Bakkt, "Introducing Bkkt: Bringing Trust and Utility to Digital Assets," accessed [2/19/2019], https://www.bakkt.com/index.

[19] William Hinman, "Digital Asset Transactions: When Howey Met Gary (Plastic)," Remarks at the Yahoo Finance All Markets Summit: Crypto (June 14, 2018), available

at https://www.sec.gov/news/speech/speech-hinman-061418.

[20] Alyssa Hertig “The Sidechains Breakthrough Almost Everyone in Bitcoin Missed.” Coindesk (January 17, 2018), available at https://www.coindesk.com/sidechains-breakthrough-almost-everyone-bitcoin-missed

[21] See David Hamilton “Lightning Network Developers Tackle Privacy Concerns.” Bitcoin Lightning (March 3, 2018), available at https://www.bitcoinlightning.com/lightning-network-developers-tackle-privacy-concerns/