Bitcoin Suisse | Decrypt

August 20, 2019 | Season 1 Episode 5

Scalability – the Missing Piece

Public blockchains have the potential to reach billions of users. A key necessity for such mainstream adoption is technology that can handle large throughputs. What is the state of scalability today? And what are the different approaches towards scalable blockchains?

Written by Dr. Raffael Huber from Bitcoin Suisse Research
and Demelza Kelso Hays and Mark J. Valek from incrementum

Blockchain technology is set to become a massive game changer. Private and public blockchains have a vast array of different use cases and will transform various industries. Recent forecasts by Gartner estimate that the value added by blockchain technology for businesses will reach $176 billion in 2025 and more than $3 trillion in 2030.[1] Such an impressive global adoption by businesses alone will require blockchains to handle large amounts of transactions per second. Add to that millions of mobile phones with integrated cryptocurrency wallets[2] that are capable to interact with decentralized applications (dApps), and the case becomes clear: **Widespread adoption requires scalable blockchains**.

Especially decentralized public blockchains, however, currently still struggle to handle substantial transaction volumes. Bitcoin was flooded with transactions at the end of 2017 after its price had achieved an all-time high versus USD. This led to over 100'000 transactions waiting to be confirmed and high fees of up to $50 per transaction.[3] While traders and investors moving thousands of dollars' worth of cryptocurrency might not mind such high fees that much, it renders the system useless for small peer-to-peer payments. Around that time, Ethereum was also suffering from congestion due to a new dApp called "CryptoKitties" – collectible tokens representing digital cats. The fact that one single relatively successful dApp significantly slowed down the entire network highlighted again the importance of scalability before mass adoption can take place.

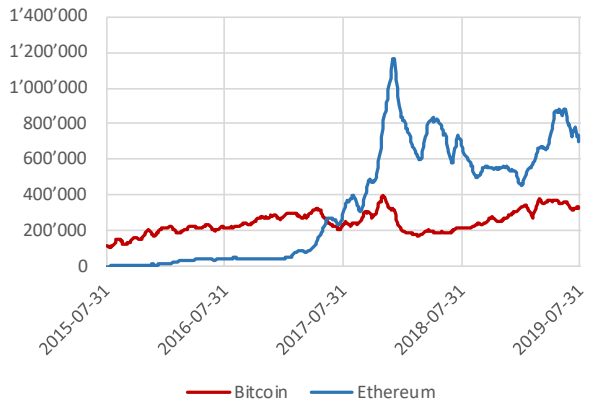
> *"I'm sure that in 20 years there will either be very large transaction volume or no volume."*
> *– Satoshi Nakamoto*

In Ethereum, miners reacted to the network occupation by a seemingly never-ending stream of virtual kitties through increasing the amount of transactions that fit into one block (i.e. raising the *gas limit*) by roughly 20%. The analogous metric in Bitcoin, the *block size limit*, has been the center of controversy for several years now and resulted in two forks: Bitcoin Cash (BCH) and Bitcoin SV (BSV). Both forks raised the block size limit by a substantial amount, increasing the amounts of transactions the networks can handle per second. The tradeoff is that running nodes becomes more expensive. Bitcoin developers chose to stick to the current 1 MB

1. https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain
2. https://developer.samsung.com/blockchain/keystore/sdk
3. https://www.blockchain.com/en/charts/mempool-count

block size limit and plan to achieve scaling in the future through second layer solutions. **In second layer solutions**, for example the *Lightning Network*, **the bulk of transactions are conducted off-chain** and only seldomly require interaction with the main blockchain. This reduces the load that the main chain has to handle.

Illustration 1: Daily transactions chart for Bitcoin and Ethereum. Data smoothed with a 21-day rolling average.



Source: blockchain.com, etherscan.io, Bitcoin Suisse Research.

Bitcoin and Ethereum currently process around 4 tx/s (transactions per second) and 8 tx/s, respectively, resulting in roughly 350'000 and 700'000 transactions per day (Illustration 1). Bitcoin protocol upgrades (such as *SegWit*) allowed to increase its theoretical limit to around 20 tx/s – however, this on-chain capacity is still orders of magnitude away from e.g. Visa (up to 56'000 tx/s). Developers of novel distributed ledger technologies claim to solve the scalability issue through a variety of protocol alterations, such as different consensus mechanisms. For example, Facebook's Libra promises 1'000 tx/s at launch, and delegated proof of stake chains such as Cardano and EOS claim to achieve 250 and 4'000 tx/s, respectively. However, until we see those numbers put to the test by a large userbase interacting with the blockchain at such rates, such numbers remain theoretical and should be taken with a grain of salt.

Should We Achieve Adoption On-Chain or Off-Chain?

On-Chain Scaling. A commonly held opinion within the Bitcoin space is that Bitcoin is useful for online commerce transactions between *individuals*. Let's take a look at what becoming digital cash would mean for Bitcoin. Online transactions comprise mostly of B2B and retail e-commerce, peer-to-peer payments, and bill pay. Approximately 3.7 billion people or half of the world's population will make a digital payment this year.[4] Digital payments are estimated to have a transaction value of $4.18 trillion in 2019, and the total number of transactions in 2018 was approximately 38.5 billion.[4]

If we assume a maximum of 7 transactions per second on Bitcoin, this roughly equates to 31.5 million transactions per year. That means, Bitcoin's network would need to process roughly 1'000 times more transactions per year in order to satisfy the demand for online payments. With an assumed velocity of 8.45[5] and a compound annual growth rate in online payment transaction value of 12.8 %,[4] John Steward Mill's Equation of Exchange formula would estimate Bitcoin's price to be over $50'000 per coin. This refers to the unlikely case that Bitcoin takes over 100 % of the market for digital payments by 2025.

Table 1: *MV = PQ* Equation of Exchange formula for forecasting Bitcoin's price.

Market Data: Digital Payments	
Total Addressable Market for Online Transactions 2019 [Millions USD]	4'137'523
CAGR	12.80% *
Last Year to use CAGR	2024 *
Velocity	8.45 *
Adoption Curve	
Base Year	2019
Market Saturation [%]	100% *
Start of Fast Growth [hits 10%]	2020 *
Take Over Time [to capture 90%]	5 *
Network Fundamentals	
Start Currency Supply [millions]	17.719
Inflation Schedule [%]	656'250 new bitcoins introduced each year, halving every 4 years
Investor discount rate [%]	30% *

* Estimated values based on assumptions.

Source: statista.com, Incrementum AG.

4. https://www.statista.com/outlook/296/100/digital-payments/worldwide
5. Based on internal calculations of average annual velocity using on-chain transactions and USD turnover from 2009 to 2019.

However, Bitcoin taking over 100 % of the digital payment market is impossible. In order to increase the number of Bitcoin's on-chain transactions, we would need to give up some of Bitcoin's security. This would allow the Bitcoin network to process more transactions per second and for a negligible fee. As we mentioned in the second edition of the Bitcoin Suisse Decrypt,[6] Bitcoin's solution to the double-spend problem relies on each user being able to easily store a copy of the blockchain. If 38.5 billion online transactions were recorded in the blockchain every year, storing a copy would become too expensive for the average user, and the security of the network would decrease.

Off-Chain Scaling. One of the earliest Bitcoin adopters, the late Hal Finney, argued that Bitcoin is better suited to be a reserve for bank-issued certificates instead of digital cash.

His theory is based on the gold standard. Historically, banks could issue gold certificates with their unique logo on them, and then banks that trusted other banks would trade the certificates on a 1:1 basis with other banks that they "trusted." For example, Bank A would issue 1'000 gold-backed certificates that could be converted directly into gold. Bank A customers could travel to other towns and use them as a valid means of payment as long as the other merchants and banks recognized the logo of the issuing bank. Other banks agreed voluntarily to accept other banks' banknotes on a 1:1 basis because they wanted their own customer to be able to transact easily in other towns and with customers from other banks. The same could be done with Bitcoin, at least hypothetically.

In that case, Bitcoin would be predominately held by banks; although, individuals would also have the option to store Bitcoin on their own. Digital payments would work the way they do now, except Visa, Venmo, PayPal, WeChat, and other payment processers would be using dollars, euros, and Swiss francs convertible into Bitcoin instead of being convertible into nothing.

With the current technology, high security means a high hashrate, which means high fees, which means Bitcoin is not suitable for thousands of on-chain transactions per second. However, advancements in cryptography and distributed computing may enable more transaction throughput without sacrificing security. In future episodes of Bitcoin Suisse Decrypt, we will dig deeper into these new emerging technologies and the different coins that implement them.

> *"I see Bitcoin as ultimately becoming a reserve currency for banks, playing much the same role as gold did in the early days of banking. Banks could issue digital cash with greater anonymity and lighter weight, more efficient transactions."*
> *– Hal Finney*

6. https://www.bitcoinsuisse.com/research/the-recipe-for-trustlessness

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

in collaboration with

incrementum