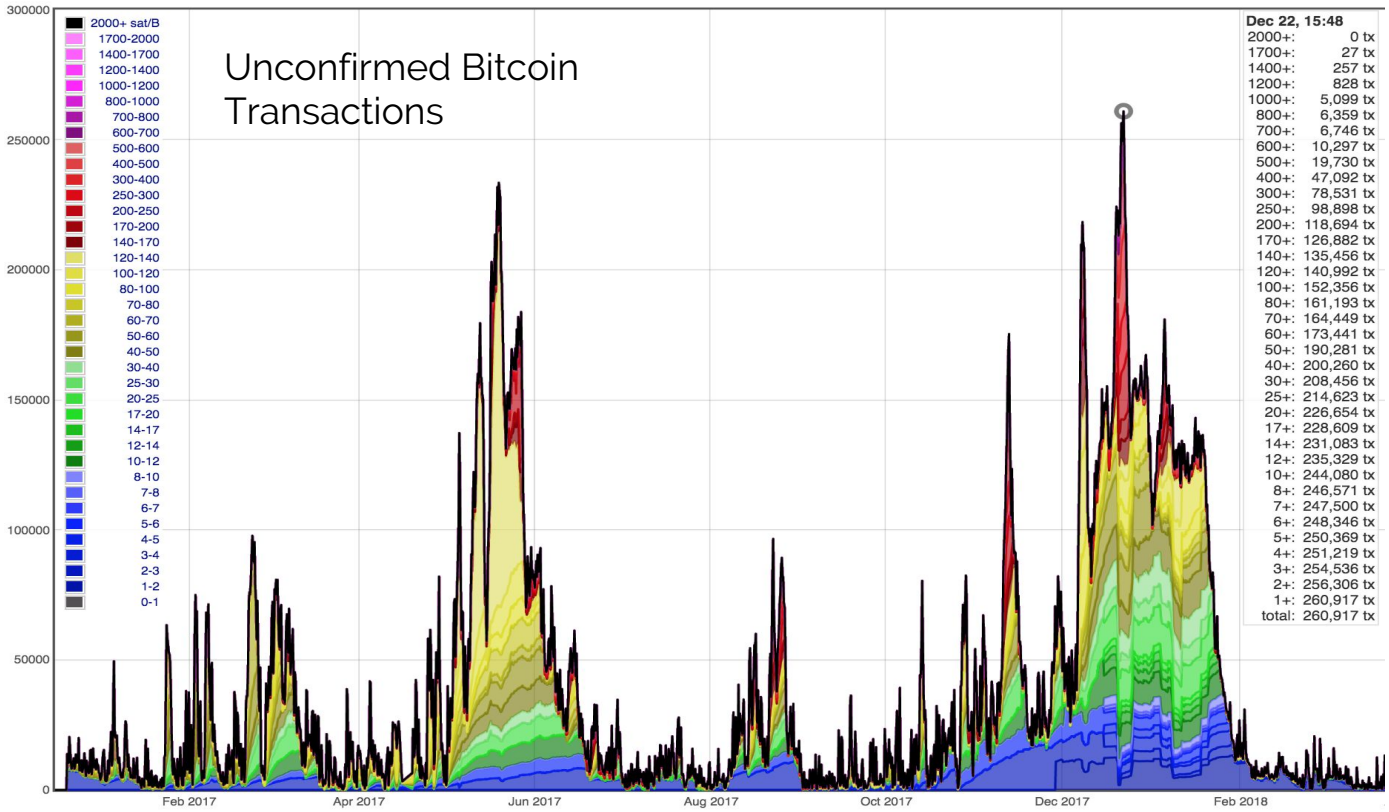
RESEARCH REPORT

# Scaling Solutions

INTELLIGENT TRADING

## Scaling Solutions

Date: 03-September-2018




The chart above is a visualisation of the Bitcoin Mempool, a memory pool of unconfirmed transactions. The numbers on the right side show the insane peak at the end of last year when there were 260,917 transactions waiting for confirmation. This is an example of the most widely used blockchain platform, Bitcoin, beginning to reach its near-capacity limits. This is the clearest demonstration of the issue of scalability.

## Strengths & Opportunities

- Scalability solutions are built on already established blockchains, either as new layers implemented on top of Ethereum and Bitcoin, or as altcoins further improving their parent chains
- There are significant opportunities for smaller chains to offer an alternative to the crowded established chains and there is an immense demand for faster and cheaper transactions
- A more scalable solution can pave the way for the mass adoption of cryptocurrencies

## Weaknesses & Threats

- Virtually all scalability solutions come with tradeoffs in security and decentralisation
- The altcoins focusing on scalability often lack other features that would distinguish them from more established cryptocurrencies. Once their parent coins solve the scalability issue, they will lose their competitiveness
- New solutions are emerging with a potential to threaten the very structure of the blockchain

# Stable Coins

**The Issue of Scalability**
- How the Blockchain Works
  - Blockchain Basics
    - Block
    - Chain
    - Size of Blockchain
  - Nodes and Trustless System
  - Forks
- Consequences of the Scalability Issue

**Solutions for Scalability**
- Techniques to increase scalability
  - Level One Solutions
  - Level Two Solutions
- Scaling solutions in the main coins
    - Bitcoin scaling solutions
    - Ethereum scaling solutions

**Altcoins for Scalability**
- Coins focusing on Scalability
  - Bitcoin Hard Forks
  - Centralizing Block Production
  - Universe Of Many Chains

**Strategic Analysis**
- Strengths
- Weaknesses
- Opportunities
- Threats

**Conclusion**

# The Issue of Scalability

## How the blockchain works

The cryptocurrencies are getting more and more attention. One of the main premises behind Bitcoin was to enable a decentralized, fast and inexpensive method to transfer value. However, with the user base constantly growing, issues of scalability have presented themselves in Bitcoin's current form. To explain the origin of this issue, it is important to understand how the blockchain works and what limitations exist in the technology that drives cryptocurrencies such as Bitcoin.

### Blockchain basics

Blockchain is the buzzword of the year 2018 according to The Guardian. The technology behind virtually all cryptocurrencies and the digital, chronologically updated distributed and cryptographically secured ledger. To describe the basics of this technology, we will take it apart and focus on what the "Block" stands for and what is hidden behind the "Chain".

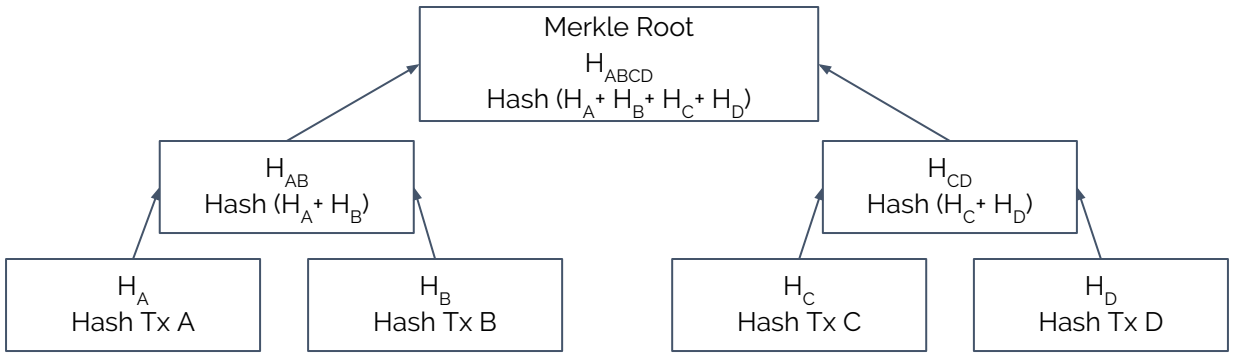
Block

The block in blockchain represents a group of transactions carried out at a point in time. The header of each block contains a cryptographic hash to the previous block, metadata of the mining competition (timestamp, difficulty, and nonce) and the transaction data. After the header, the list of transactions follows.

| Header hash |
| --- |
| Header hash of the previous block<br>Mining metadata<br>Merkle root summarizing all the data in the transactions |

To summarize the transaction data, Merkle trees are used. Those binary hash trees create a digital fingerprint of the entire set of transactions. As per Andreas M. Antonopoulos, Merkle trees are used as a means of "efficiently summarizing and verifying the integrity of large sets of data".

The node on the top is the Merkle root, calculated by pair-wise hashes of the nodes. The figure below shows a Merkle tree consisting of four transactions, A, B, C and D. The leaf nodes are paired so there needs to be an even number of them. In case there is an odd number, one of them is duplicated to create a balanced tree.




The Genesis Block of Bitcoin blockchain contains one transaction and is the first brick of the whole blockchain and it's timestamped to 2009-01-03 18:15:05. The reward for this block was 50 Bitcoins and it contained the note "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" marking the time the block was created and also a referencing to instability which is caused by fractional-reserve banking.

The Genesis Block is at the inception of all blockchains at the block height 0. Subsequent blocks are added on top of this block and currently, the Bitcoin blockchain has reached the height of 540,018 blocks. Those blocks are linked in chronological order and create the Chain.

# The Issue of Scalability

Chain

The chain of blocks in the blockchain are linked together in a linear, chronological order and refer to the previous block. The distributed network decides if the next block should be added to the blockchain based on consensus. The consensus used in Bitcoin is based on solving a complex mathematical puzzle and depends on the amount of processing power invested in the network in a Proof-of-Work algorithm.

The trustless verification of blockchain relies on the principle of immutability. This is based on the fact that any change within a block modifies the value of its hash (fingerprint). It does not mean that the data can't be changed, but that it is extremely difficult to change it without serious collusion, and if somebody were to try, it would be extremely easy to detect the event. The bigger the size of the the blockchain (the more blocks there are), the harder it is to rewrite it.

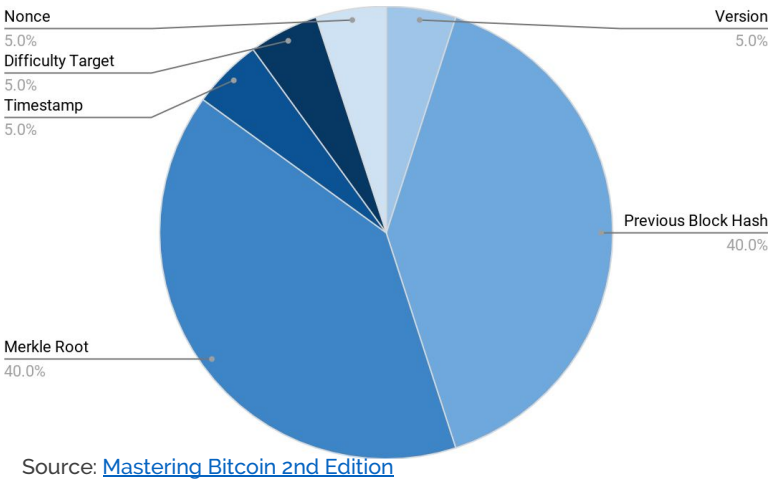
Blockchain Size

The size of the blockchain depends on the amount of data each block contains. We have described the structure of a block, consisting of the block header and the list of transactions. The main proportion of the block size is made up by the transactions. Looking at the structure and the size of each part in bytes in ascending order:

| Part of block | Size | Description |
|---|---|---|
| Transaction Counter | 1-9 bytes | Shows how many transactions follow after the header |
| Block Size | 4 bytes | Shows the size of the block in bytes |
| Block Header | 80 bytes | Header hash of the previous block, mining metadata and the merkle root with transaction data |
| Transactions | Variable | The transactions recorded in the block (average transaction is at least 400 bytes and the average block contains around 2,000 transactions) |

Source: Mastering Bitcoin 2nd Edition

If we look closer at the block header structure, we can take it apart and assess the size of each group of metadata. On the right, there is a graph showing the structure and proportional size of: *Nonce*, a counter used for the Proof-of-Work algorithm, the *Difficulty Target* which shows the Proof-of-Work algorithm difficulty for this block, a *Timestamp*, the approximate creation time of this block and a *Version* number that tracks the software protocol upgrades. Each of these four parts has approximately 4 bytes. The *Merkle Root* and *Previous Block Hash* with a combined 64 bytes makes up the rest of the 80 bytes of the block header.

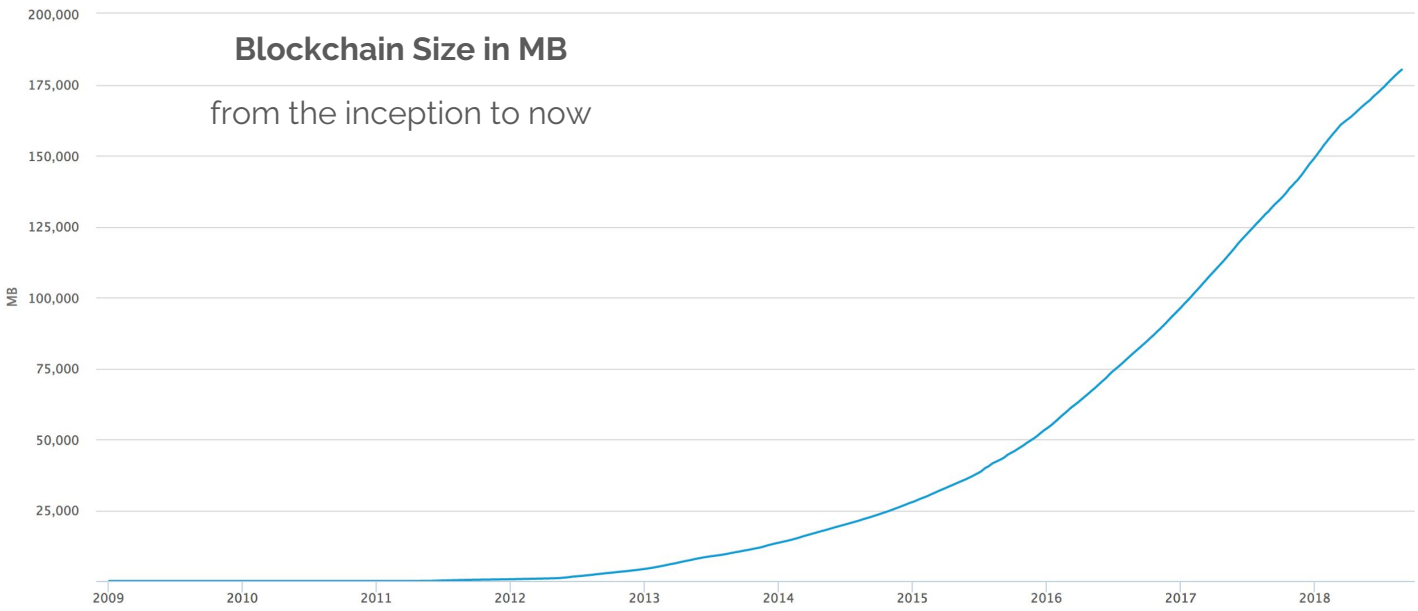



Source: Mastering Bitcoin 2nd Edition

# The Issue of Scalability

Blockchain Size - continued

There are different approaches to the block size increase, however, with the increasing number of transactions and blocks added, the blockchain is inevitably growing. The chart below shows the total size of all block headers and transactions in MB from the inception of bitcoin to now. From 2012, there is a steep increase in the growth and at the time of the report the total size of blockchain was 181,223 MB.




**Nodes and Decentralized Trustless System**

The hundreds of thousands of MB of blockchain have to be to be maintained and stored. In decentralized ledgers, this is done by a network of nodes (computers) that store a copy of the blockchain. To assure that all nodes have the same shared database, they periodically synchronize. In the Bitcoin whitepaper, Satoshi Nakamoto explained the principle of the network. Every node in the Bitcoin blockchain network has a copy of the longest blockchain and nodes only accept new blocks when "all transactions in it are valid and not already spent." To demonstrate that they accept the block, the nodes use the hash of the accepted block as the previous hash when creating the next block in the chain.

This method provides the network significant resilience. Because the same copy of the blockchain is stored by multiple nodes, even if one or more computers fail, the shared database can be recreated. The decentralization is, however, achieved at the tradeoff of a slower and less scalable system. The processing speed is limited to that of a single node that is participating in the network and as the blockchain grows, there are higher requirements for storage, bandwidth and computing power.

In order to scale the blockchain, more computing power would have to be added to every node in the network. This is possible in private blockchains, but in public blockchains, there is no way to do this.

The scalability issue causes comparable (if not more pervasive) concerns in the crypto community, especially in regards to privacy and volatility issues, which we have already addressed in the previous reports. The attempts to solve this issue lead to the emergence of new altcoins, causes disagreements among nodes in the blockchain networks and results in soft and hard forks.

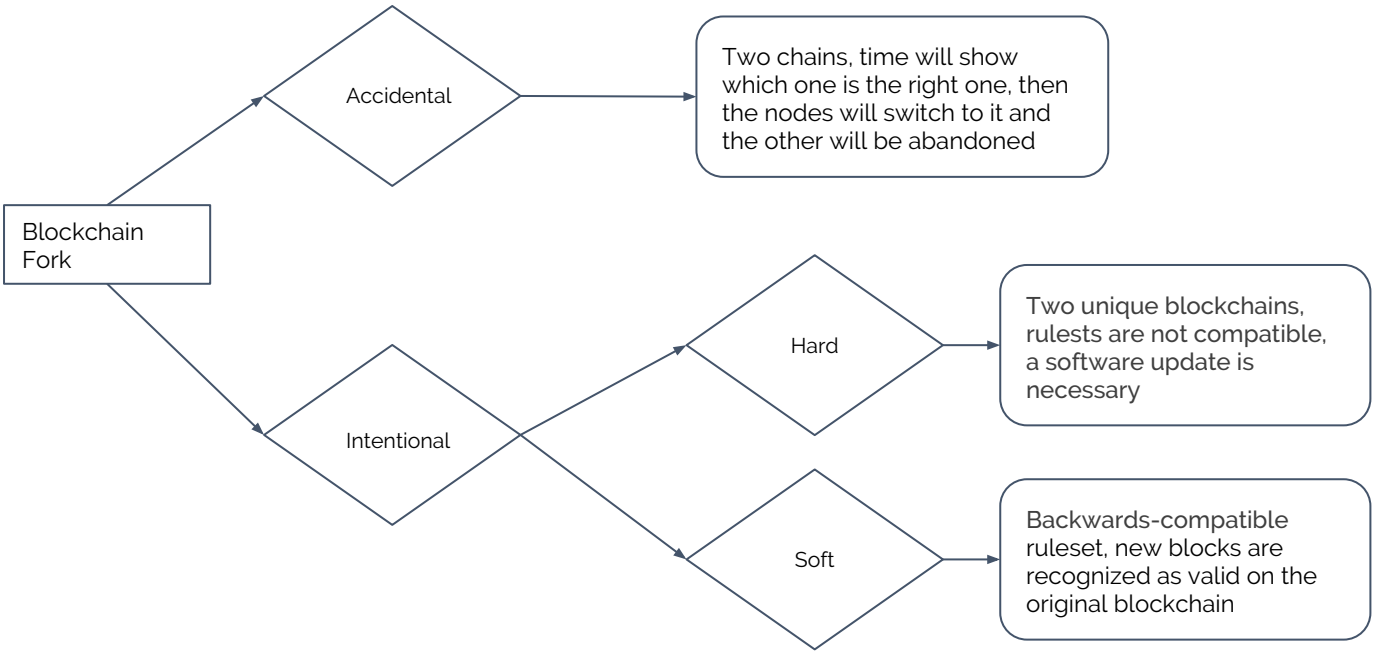
# The Issue of Scalability

### Forks

The Bitcoin blockchain served as a foundation for numerous projects. The changes to the original chain are known as forks and they can be divided into two main groups, based on different motives. In lines with how new blocks are added to the chain, a situation can occur when a number of miners create a block at nearly the same time. This leads to two chain variants, and the fork cannot be resolved until one of these new chains is longer than the alternative, and the nodes switch to that one and the "orphaned" blocks are abandoned. This is what we describe as the *Accidental fork.*

The second category is the *Intentional forks,* which occurs when there is a need/will to change the ruleset of the original blockchain. This type of fork is further divided to *Hard forks* and *Soft forks.* With the Hard fork, the new ruleset is inconsistent with the old ruleset, thus creating two unique chains from the original blockchain. Nodes can decide on which chain they want to operate, while a software update is required to work on the new chain.

The Soft forks are "backwards-compatible", so the blocks created by the fork's new ruleset are still recognized as valid by the original blockchain. The graphic below demonstrates a different kind of fork.




Currently, there have been over ninety Bitcoin forks. out of which over seventy are now active projects. Some of them are hard forks, such as Bitcoin Cash (BCH) or Bitcoin Gold (BTG) and some are airdrops issued to holders of Bitcoin (BTC). Bitcoin is also not the only "parent" coin, there are already over twenty projects forked from a major altcoin. Most of them are forks of Ethereum (ETH), followed by coins with heritage in Monero (XMR), Litecoin (LTC), NEO and also Dogecoin (DOGE) and Dash (DASH).

One of the most common reasons for a hard/soft fork of the original Bitcoin blockchain is the issue of scalability. We have outlined the reason for it, being the growing size of major blockchains and the tradeoff between the decentralization of the node network. Now we can consider the results and consequences of the issue of scalability, which will help us understand why there are so many altcoins trying to solve it.

# The Issue of Scalability

## Consequences of the Scalability Issue

The chart on page five is one example of the exponential growth of the blockchain network. It illustrate that the size of the blockchain is not the only aspect that skyrocketed over time. The number of users is also increasing, as is the tera hashes per second performed by the network, and the difficulty to find a new blocks. And as the time passes, even the major blockchains are starting to show their limitations.

In comparison to the real world applications, major cryptocurrencies are still lagging behind. The chart below shows the number of Bitcoin transactions added to the mempool (Memory Pool of unconfirmed Bitcoin transactions) on the Bitcoin network per second. The chart reaches its peak at the end of the year 2017, reaching slightly under five transactions.


Source: Blockchain.com

Although there are altcoins scaling with better results, the processing speed of the real world applications such as Visa (capable of 24,000 TPS) and PayPal (able to process more than 1,200 TPS) is still considerably higher.

The increase in Bitcoin transactions at the end of last year was not nearly enough to satisfy the demand for transaction processing. With the bitcoin price reaching its peak at the turn of this year, the unconfirmed transactions were piling up reaching as high as 200,000 and the transaction fees of as much as $54.9 have been reported on 21.12.2017. Ethereum faced similar backlog unconfirmed transactions, e.g. after the success of Crypto Kitties, a game built on the Ethereum, which exposed the vulnerabilities in Ethereum smart contracts.

For Bitcoin, the constraint is the Blocksize limit. By determining how much transactional data can be contained within this limit, an upper limit on throughput is created. In Ethereum, users pay for a smart contract execution with each block capable of carrying a limited number of execution units. This affects verification speed.

Vitalik Buterin established the issue of trade-offs in what he calls the Scalability trilemma. He addresses the issue of developing a blockchain technology providing scalability, decentralization, and security, without compromising either one.

With the scalability limitations of the popular cryptocurrencies, the higher traffic leads to increasing transaction fees, as well as delayed processing of transactions that cannot be fit in one block. That is why the major cryptocurrencies are releasing updates increasing scalability and altcoins are designing their blockchains with scalability as their goal. Below we will look at some of the solutions.

# Solutions for Scalability

## Techniques

In principle, there are several ways to increase the scalability of existing blockchains. Based on a distinction made by Vitalik Buterin, we can talk about two layers of solutions: layer one, built-in blockchain solutions; and layer two, off-chain solutions implemented on the top of existing blockchains.

### Level One Solutions

The level one solutions are based on changes to the original blockchain protocol and mostly requires a fork to be implemented. The first and the simplest solution that comes to the mind when speaking about the block limitation would be to increase the block size.

Block Size Increase

Although this seems to be a logical step, there are strong arguments against this. The block increase was one of the main debates in the Bitcoin community. In 2013, a condition in the Bitcoin protocol was discovered, hidden in two commits.

Until then, it was not taken into consideration but once it was discovered to be a no-op upper limit of the 1MB size of bitcoin block, it caused a vivid debate, especially after the spur of interest in Bitcoin in 2015. There were several advocating in favor of a hard fork and removing the limit (bitpay CEO Stephen Pair, Magnr and Coinbase CEO Brian Armstrong) but also arguments against the hard fork (Adam Back, Bitcoinpaygate and Paymium CTO David Francois).

The main argument for the block increase is that this fairly simple solution would decrease transaction fees, making it cheaper for the users. When the block is bigger, more transactions can fit in it and the miners will get a reward from more confirmed transactions in one block. On the other hand, the opponents are afraid that this could potentially disincentivize the miners, since the lower transaction fees may mean a lower reward for them.

The next contra argument is the centralization aspect of this step. With a bigger block size and a growing network, more processing power will be required for block confirmation. This will eventually push the small players out and concentrate all the mining to huge mining pools and mining farms, leading to centralization.

| Arguments in favour | Arguments against |
|---|---|
| More transaction in a block will increase the transaction output per second | With larger blocks, the network will grow bigger and make full nodes more expensive to operate |
| The transaction fees can decrease | The miners will be disincentivized by lower transaction fees |
| There is no off-chain solution ready to take off the load from the main blockchain | The larger blockchain will require more computing power and eventually will exclude smaller miners and centralize the block creation to huge mining pools |

# Solutions for Scalability

Sharding

Another level one solution, to be implemented in Ethereum, is sharding. The technique splits a blockchain into different sections called shards, each of which is stored by a different node from the network. Transactions are grouped by the shard to which they belong and nodes in each shard process parts of the information in parallel, allowing for increased speed. Below there is a picture of a single shard.

| | | | |
|---|---|---|---|
| Shard ID: | 43 | <sig #1284> | <sig #2543> |
| Pre state: | a138b3ff | <sig #7821> | <sig #6118> |
| Post state: | 835680cc | <sig #9053> | <sig #4337> |
| Receipt root: | fa3819d4 | <sig #1662> | <sig #4785> |

Transaction group header

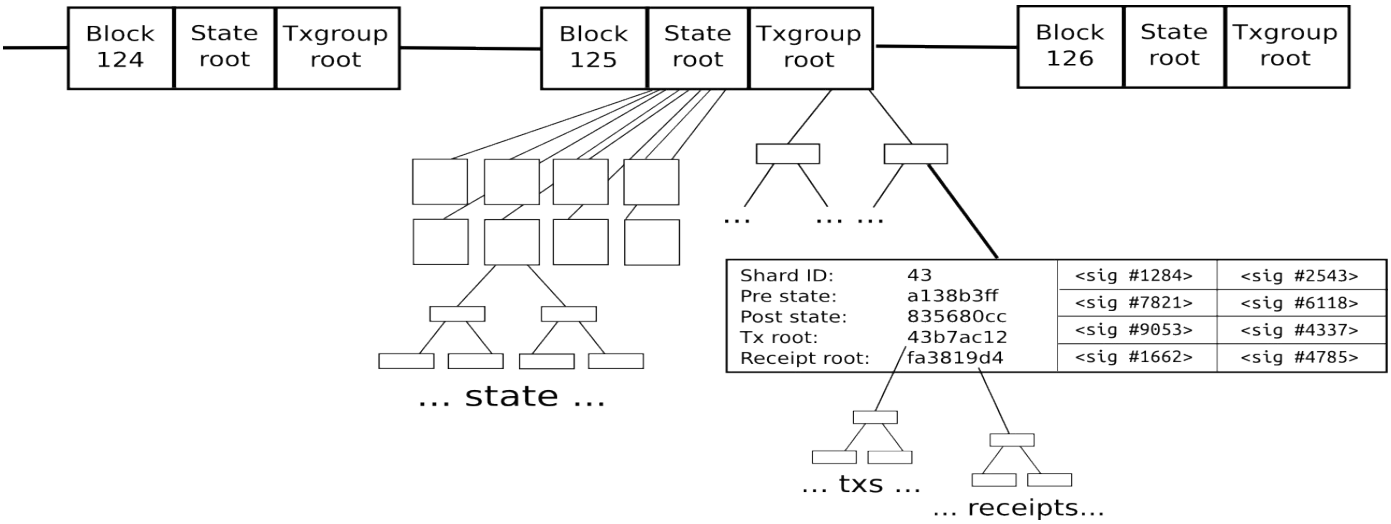
| | | |
|---|---|---|
| Tx a142 | Tx a558 | Tx eca6 |
| Tx a35f | Tx e25a | Tx 34ac |
| Tx 2308 | Tx 6987 | Tx f260 |
| Tx 9f14 | Tx ec30 | Tx 5fc3 |

Transaction group body

Every transaction specifies the transaction ID in the top right. The pre-state describes the situation before the transactions were applied, post state after it. Each transaction belonging to shard X implies that it sends from and to an account in that respective shard. The blockchain then on a level two accepts the group of transactions rather than single transactions. This enables lots of parallel transactions to happen and at the same time and increases the performance.

Source: Scalability and Asynchronous Programming

The following diagram demonstrates the normal blockchain with two roots, the state root (entire state, a set of information that represents the "current state" of a system) and the transaction root (all transaction groups in the blockchain).




The cross-shard communications can be implemented in different ways, Ethereum follows the receipt paradigm when every transaction in shard generates a receipt, representing an effect of a transaction stored in a Merkle tree. They can be viewed by other shards, but not modified by them.

Sharding can be an effective solution but comes with several challenges. The system requires a mechanism to assure that the shards completed the work on their part of transactions, a way to enable communication between the shards and a method to assure fraud detection.

Due to the structure of the sharding method, it's easier to compromise the system by compromising a single shard within that system. Based on an article by Vlad Zamfir, it is easier to attack shards with lesser hashrate in the Proof-of-Work systems (such as Bitcoin). That is why sharding makes more sense in Proof-of-State consensuses. Partial proof-of-concept was released for Ethereum in May, but the final release for sharding will not come sooner than in 2020.

# Solutions for Scalability

### Level Two Solutions

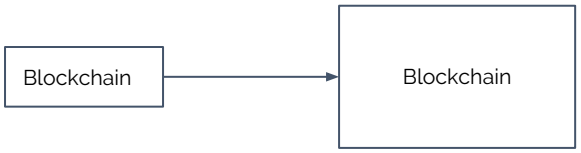
The level two solutions are built on top of existing blockchains and do not require a hard fork to be implemented, unlike the level one solution. They are compatible with the original version of blockchain and send most of the transactions off-chain. The level two solutions only interact with original blockchains when there is a need to enter and exit from the layer-2 system and in case of an attack on the system.

The idea behind the level two solution is that the method does not increase the capacity of the blockchain itself, as the base-layer throughput stays the same. The solution aims to do more operations thanks to performing some of them off chain, while still remaining secure. In case of Ethereum, those solutions exist in the form of smart contracts, that interacts with the original blockchain.

The second layer solutions are using the cryptoeconomic consensus of the underlying blockchain (Ethereum, Bitcoin) as a fixed point to which they can attach additional mechanism and solutions, referring back to the anchor of original consensus.

Level One Solutions

Increase the blockchain scalability by increasing capacity of the base blockchain.




n TPS n*X TPS

Level Two Solutions

Increase the effective transaction throughput by performing some operations off-chain


n TPS n*X TPS

The main level two solutions can be further divided based on the base protocol they are implemented on. Further below, we will focus on the way the two major coins, Bitcoin and Ethereum work with both levels of solutions.

| Level One Solutions | Level Two Solutions |
|---|---|
| Requires a fork from the original chain | Does not require a fork to be implemented |
| Change on the base-layer of the protocol level | Change compatible with the original blockchain, can run on top of it |
| Maintain simple protocol design and decentralization | Comes with more complicated cryptography and technical solution |
| Examples on Bitcoin: Block Size Increase | Examples on Bitcoin: SegWit, Lightning |
| Examples on Ethereum: Sharding | Examples on Ethereum: Plasma, State Channels |

# Solutions for Scalability

## Scaling Solutions in the Main Coins

### Bitcoin

Even though there is currently already 1910 projects and altcoins, Bitcoin still owns a significant market share and dominates the cryptocurrency market with 53.24%. That is why we have used Bitcoin to illustrate the issue of scalability, as Bitcoin as the flagship of cryptocurrencies is the one that has to deal with the highest number of users and transactions. Currently, there are two main approaches to level one and level two solutions. On the first level, it is the block size increase that is discussed the most.

Block limit debate

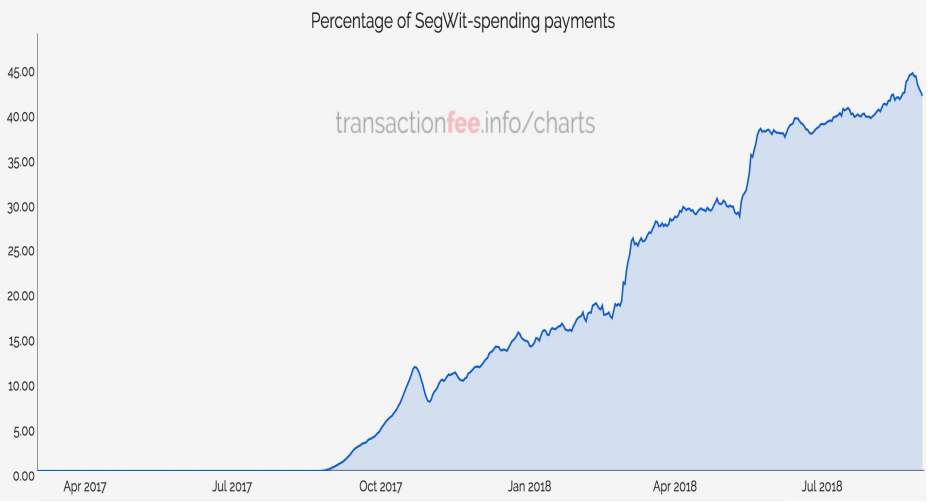
The original limit to the Bitcoin block size to 1MB was implemented in blockchain in 2010 when the cryptocurrencies landscape was quite different to what we have now. Theymos, administrator of both the Bitcointalk forum and bitcoin subreddit commented on the state at that time, saying that no one had anticipated mining pools would happen, or ASIC mining, which caused a mining centralization. It would seem that Satoshi realized later after the introduction of Bitcoin that there was a danger of miners creating blocks larger in size than other miners would accept, leading to Denial of Service attack. The limit of 1MB may seem reasonable back in 2010, but failed to provide the necessary speed when Bitcoin gained greater popularity.

After the condition was discovered, a debate about increasing the block size begun. It was at this time there were several attempts to increase the block size. In 2015, there were the first two proposals, BIP 100, (making the block size limit adjustable at the miner's decision) by Jeff Garzik and BIP 101 (a one time increase from 1MB to 8MB) by Gavin Andresen. Neither of those has been realised

After that, several proposals followed (Bitcoin XT, BIP 102, BIP 103, Bitcoin Classic and Bitcoin Unlimited) until one of them was implemented. The final deployed solution was SegWit, or Segregated Witnesses.

SegWit

SegWit was proposed in December 2015 by Pieter Wuille, Blockstream co-founder and developer. It works on the principle of separating the signature data (the "witnesses") from the transactional data. SegWit can take data from the core Blockchain and store it elsewhere. By doing this, it is possible to increase the overall block size to 2-4 MB. SegWit was activated by BIP143 on August 24, 2017 as a soft fork of the core protocol, as of block height 481,824.




As the graphic shows, right now, there is approximately 45% of miners using the SegWit transactions. SegWit increased the number of transaction in one block by reducing the size of individual transactions. On the other side, miners get lesser fees for the individual transaction. The implementation is also quite complex, all the wallets will need to implement SegWit themselves. Also, the sidechain has to be maintained by miners as well.

Source: transactionfee.info

# Solutions for Scalability

Lightning network

Even more highly anticipated than an increased block size was the base SeqWit created for a second-layer technologies like the Lightning network. Joseph Poon and Thaddeus Dryja proposed in their whitepaper an off-chain micropayment system, which allows for executing smart contracts off chain.

The lightning network sets up a multisignature wallet and a saving wallet address in the blockchain. Parties then execute transactions without having them public on the blockchain and after all transactions are completed, the resulting balance is saved in the blockchain, and parties involved can recover their share from the wallet. The time-lock mechanism allows for transactions to be committed to a blockchain and broadcast at a later time.

The Lightning Network is making microtransactions possible, as there is no need for custodian fees and the off-chain solution enables near-instant micropayments. However, there are still some limitations, lightning is still a work in progress, the first mainnet release was announced in March 2018. The main issue is that it is not as safe as Bitcoin, so the utilisation is mainly for microtransactions.

**Ethereum**

We have already described the method of sharding, which is the level one scaling solution utilized in Ethereum. As per Vitalik's post from this January, Ethereum aims to combine the layer one and layer two solutions and views them as complementary with each other. So what level two systems already exist for Ethereum?

State Channels

The state channels solution is also working with conducting some operations off chain. It was first described in November 2015 by Jeff Coleman and works with the mechanism of creating a payment channel (similar to the lightning network). The payment channel is opened on chain, while the opening costs a standard fee and takes the standard verification time on the Ethereum blockchain. Tokens are locked up in the payment channel smart contract and transfer between parties on the blockchain cannot be higher than this locked-up deposit.

The transactions are happening off chain and are submitted to it when there is a final state (balance). To illustrate this, we can imagine party A and party B sending each other blockchain-certified cheques with no actual cryptocurrencies changing owner up to the point when they decide to broadcast it on the public blockchain. At that point, each party has a stack of cheques which they can use whenever they want and redeem their share of the locked-up deposit.

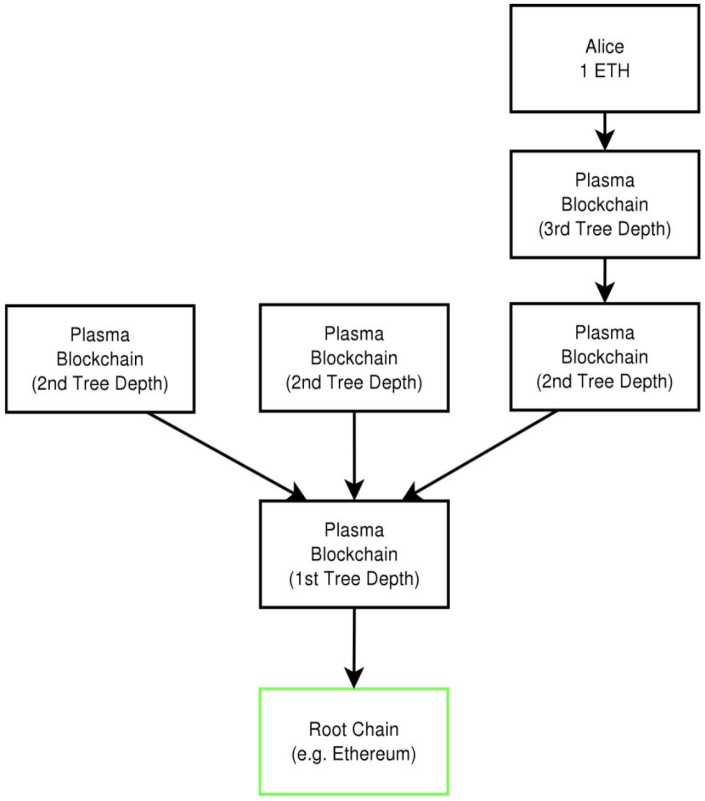
The parties pay only one transaction fee for submitting the final list of all transactions conducted. After submitting, there is a waiting period which ensures that no one can legitimately challenge the final result. This period is important e.g. in the case when party B send an old version of the transaction list, where there are missing transactions it owes to party A. In this waiting period, party A can prove that party B is not honest and send an updated version of the list.

The state channels improve the scalability by conducting off chain transactions, however, there is some trade-off to this solution as well. The solution depends on availability, if the party A is not available and online, it may not be able to correct the party's B false statement before the waiting period ends. The state channels usefulness is also limited by the number of transactions sent. Due to the initial cost to create the smart contract, it is not profitable for sending just a few transactions. And lastly, the smart contracts need to know the parties involved (addresses), so this solution is useful for transactions with a defined set of participants.

# Solutions for Scalability

Plasma

Joseph Poon is also a co-author of another scaling proposal, Together with Vitalik Buterin, they released a paper called Plasma: Scalable Autonomous Smart Contracts in August 2017. In this paper, they have introduced the concept of a series of contracts running on top of the Ethereum blockchain. It works on a similar principle as state channels, conducting the transactions off chain, but increases the scalability potential by creating "child chains" attached to the root Ethereum blockchain. These "child chains" can continue creating their own "child chains" and so on.




Source: Plasma whitepaper

The picture on the left demonstrates the tree hierarchy of the root chain and the child (Plasma) chains. Only blockheader hashes are submitted to the root chain and the Plasma chains act as separate blockchains. This allows for high scalability, as the root chain process only a small amount of data from the child chains.

The operations on the Plasma chains do not need to be replicated across the entire blockchain, so the transactions can move faster and they can be cheaper. The security of the system is assured by using the Fraud proofs (mathematical proofs used to make sure that a block is valid) to enforce invalid blocks.

The linkage to the root chain offers a safety net, due the fact that if there is an attack on a particular chain, the parties involved can exit to the root chain. A significant advantage of Plasma is that it can even implement state channels solutions like Lightning network on top of Plasma.

Unlike in state channels, not all participants need to be online in order to update the state and they do not need to do the final submission of a list of transactions in order to confirm those transactions. State channels are, on the other hand, faster and less expensive per transaction, given that there is a significant number of transaction carried out within the payment channel.

The Plasma solution is also in an early stage of development. At the beginning of the year, Vitalik proposed a stripped-down Plasma implementation called Minimal Viable Plasma.

Other Solutions

As the scalability solutions for Ethereum are still under development, there are more methods and proposals. For example, TrueBit, designed for complex computation off-chain, will not improve the transaction throughput but enable scalable transactions among Ethereum smart contracts. As proposed in the whitepaper, TrueBit introduces the concept of paying a small fee to a *solver* to do the computation off chain. The trust is enforced by smart contracts and uses a mechanism called "verification game", involving *challenger* to check the solver's work.

# Altcoins for Scalability

## Coins focusing on Scalability

One of the alternatives to increase scalability of existing blockchains it to assume that when users are faced with higher transaction fees and longer verifications times, they will opt out from major cryptocurrencies and look for altcoins who provide better terms of transaction execution.

The main idea behind this approach is that with more altcoins, users can choose some of the less established ones and this will take the load of the Bitcoin and Ethereum blockchain. Smaller cryptocurrencies sure do promise better scalability, but mostly comes at a cost of security. As we already covered in our previous reports, there are altcoins focusing on different aspects of different cryptocurrencies' characteristics. Scalability is vital to all cryptocurrencies, so there are attempts to solve the scalability issue in virtually every project, however, there are several projects that set scalability as their main focus.

### Bitcoin Hard Forks

When Bitcoin gained broader popularity, it was obvious that the scalability of the network was not sufficient. The first altcoins originated as an attempt to solve some of the issues of their core currency, and emerged as a fork of the Bitcoin Core protocol. One of the first altcoin was Litecoin.

Litecoin (LTC)

Litecoin was launched in October 2011 by Charles Lee, a software engineer at Google. It was nearly identical to the of the core protocol. The main difference was the decreased block generation time (2.5 minutes), an increased maximum number of coins (84 million) and a different proof-of-work algorithm (scrypt). In comparison to Bitcoin, its parent currency, Litecoin is cheaper, both to transact (lower transaction fees) and to mine (lower entry costs, can be mined even with CPUs). In respect to mining, Litecoin is also less ASIC resilient than Bitcoin, due to higher requirements for memory per hash. The mining difficulty adjusts to make sure that blocks are released every 2.5 minutes, which leads to faster and more reliable confirmation time.

On the other hand, the Litecoin solution is less secure in comparison to Bitcoin, it provides less security from attacks that rely on lowering the difficulty and assure weaker security guarantees due to the fact that less computing power is necessary to generate new blocks. According to Lee, Litecoin is intended to complement Bitcoin payments. Bitcoin would be the more valuable, more secure and more expensive digital gold, used for storing the value, whereas Litecoin would serve as the digital silver, cheaper and better suited for day to day payments.


Bitcoin Cash (BCH)

Bitcoin Cash is the product of the block limit debate, originating in August 2017 at the block 478,558. Holders of Bitcoin had access to the same amount of Bitcoin cash at the time of the fork. The main difference was the block size, originally increased to 8MB and currently, Bitcoin Cash supports blocks as big as 32MB.

The combination of lower demand and bigger blocks gives Bitcoin Cash superior scalability over Bitcoin, however, the question is how long this will possible. The increase from 8MB to 32MB can prevent filling the blocks with higher demand, however, BCH did not implement segwit to prepare for lightning, so the block size increase is its main strategy for scalability. Already at 8MB, Bitcoin Cash was able to support 40-90 transactions per second. However, we have already covered some of the disadvantages of using increasing block size as the solution for scalability, including the large size of the blockchain and disincentivized miners.

# Altcoins for Scalability

## Coins focusing on Scalability

### Centralizing Block Production

Another group of altcoins focusing on scalability are based on the proof-of-stake consensus and implement its variant, DPoS, delegated proof-of-stake. This algorithm is based on the concept of blocks being validated not by the token holders but rather by "witnesses". These "witnesses" are elected to validate blocks on behalf of the token holders. This leads to a certain level of centralization in the block creation. The effect of limiting the number of block producers is that each of them can accumulate more resources.

Eos (EOS)

Eos is the most prominent project of Dan Larimer, the inventor of the DPoS algorithm, and it has publicly revealed that there will be only 21 block producers at a time (one of them, mining company Bitmain). It positions itself as a competitor of Ethereum in creating an infrastructure for decentralized applications. The platform promises to eliminate the transaction fees and conduct a million transactions per second. As the project gains significant popularity, currently ranking fifth on CoinMarketCap, and there is some controversy about the technology, we decided to dedicate one of the next deep dive research reports to further analysis of this project.


Cardano (ADA)

Cardano is another one of DPoS project, started in 2015 introducing two protocol layers to separate accounting and computation. We have conducted and published a research report with both fundamental and technical analysis of the project earlier this year.

### Universe Of Many Chains

There are several projects that believe that instead of monolithic chains, such as Ethereum or EOS, there will be a hundred or thousand of different chains. This leads to the idea that different applications do not need to share a single set of validators. Instead, they can each have their unique validator sets.


Cosmos (ATOM)

The Cosmos project aims to create an internet of blockchains, using Ethermint to spin up new chains and fostering interoperability among the chains. Cosmos achieves scalability through vertical and horizontal approach. The vertical approach provides more shared resources to the operating system and applications and the horizontal approach is achieved by multiple parallel chains running the same application.

The architecture is based on several independent blockchains, so-called "Zones" which are linked to a central blockchain called the "Hub". The Hub is secure by a globally decentralized group of validators. This application-specific blockchain is still in an early stage of development and its novel technology (Tendermint PoS) is yet to be proven in the market.

# Strategic Analysis

### Strengths

The main strength of scalability solutions is that they all build on what is already there. In a more literal sense, there are the second layer solutions that aim to increase the scalability of existing coins and further improve a coin that is already established and has a strong user base.

The altcoins alternative are riskier, but they all also build on their parent currencies, taking what is best in them. The fact that scalability is the crucial focus of a significant number of developers in the cryptocurrencies ecosystem also assures an advanced technology and interest of both users and investors.

### Weaknesses

Virtually all solutions we have covered above come with some sort of tradeoffs. Vitalik Buterin addressed this in his Trilemma and all the projects we have covered are to some extent victims to the necessary tradeoff of either security or centralisation. In order to achieve higher scalability, the projects have to sacrifice some advantages, so in comparison to e.g. privacy coins, the coins focusing on scalability are not able to achieve a high level of security or anonymity of their users.

Each of the altcoins solutions has their respective weaknesses and disadvantages, e.g. the centralisation connected to the block increase in Bitcoin Cash or the lower security of Litecoin. Their common weakness is that in general, they do not offer any superior feature over the established coins other than scalability, and this makes them vulnerable in case of Bitcoin or Ethereum solving the scalability issue on their own.

### Opportunities

When talking about the consequences of the scalability issue, we have demonstrated that there certainly is a potential for a more scalable coin or for a solution to increase the scalability of the established giants. With the increasing interest in cryptocurrencies, the limitations of existing coins is obvious.

The fact that smaller user base generally leads to higher scalability also poses an indisputable opportunity for smaller chains and altcoins. Every backlog in transaction processing in Ethereum and Bitcoin is an opportunity for the altcoins to offer lower fees and faster verification for those who do not dwell on the robust security of established chains.

### Threats

When talking about the threat to scalability solutions, there are different points of view. For the altcoins, the obvious threat is the scalability solutions in their parent established blockchains with larger user base. And for Ethereum and Bitcoin, there is the potential threat of a whole alternative solution which is not based on their parent blockchain, DAG, Directed Acyclic Graph as implemented in IOTA or Spectre.

Directed Acyclic Graph of transactions where anyone can add their own transactions using PoW, pointing to two previous transactions is an alternative to blocks in the blockchain. This novel approach promises better scalability and limitation of transactions fees.

# Conclusion

In this report, we have not nearly covered all of the solutions for scalability. We aimed to provide you with an introduction to the scalability issue. The goal was to explain why it is important to search for the solution, and then offer you some examples of how the major coins are progressing and competing with altcoins.

There are also other opportunities as well, and we have outlined some of these (bulletproofs, zkSNARKs etc.) in our previous report. In general, it is important to note the significant role scalability issue play in project valuation and to be familiar with the basics as the coin that provides the highest scalability will likely be the most suitable for mass adoption.

# Be confident about your next cryptocurrency trade

Intelligent Trading Foundation provides you with concise cryptocurrency trading insights so you can make the right trading decision, every time. Take advantage of upside movement, and help manage downside risk.

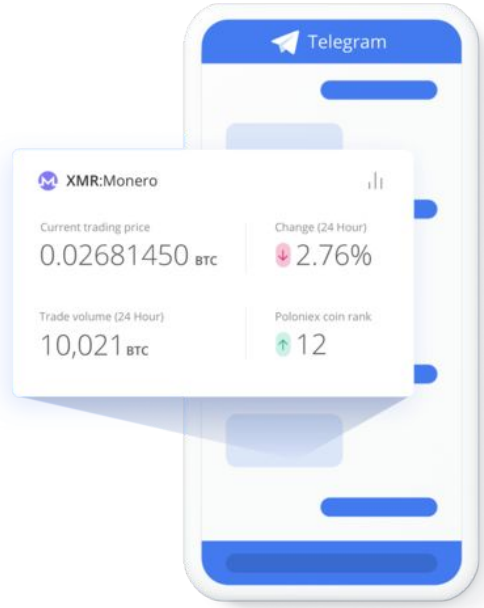
## Get real-time notifications when the market is trending

Our Telegram Bot monitors thousands of real-time data points, identifies opportunities using machine learning algorithms and technical analysis, then provides you with actionable alerts you can trade on.

**Act on every opportunity**
Our technology does all the grunt work so you can focus on making trades, instead of sorting through massive amounts of data.

**Protect your downside**
We inform you when the market is trending up, and when it is trending down, so you can minimize your risk and maximize profit.

**Easy to understand**
The alerts you receive are concise so you will immediately know what action to take, even if you are new to crypto trading.




**Make sense of all the noise with easy-to-understand crypto trading alerts. It's the smart way to trade cryptocurrency.**

**Get free access to the ITF Telegram Bot today!**
Visit https://intelligenttrading.org to learn more.

# Disclaimers

ITF, is engaged in providing trading services to the cryptocurrency trading market. Through its bot and other services it alerts its subscribers/followers ("Users") to certain market conditions based on those Users' preselected settings and trading preferences. Additionally, ITF does make available, from time to time, written or electronic communications that include research analysis, and/or a opinions concerning the DLT/cryptocurrency markets ("Reports"). The views expressed in such Reports are based solely on information available publicly/internal data/other sources believed to be true. The information is provided merely as a complementary service and do not constitute an offer, solicitation for the purchase or sale of any financial instruments, inducement, promise, guarantee, warranty, or as an official confirmation of any transactions or contract of any kind.

Research data and reports published/emailed/Telegrammed/etc. and or those made available/uploaded on social networking sites (e.g. Facebook, Twitter, LinkedIn, etc.) or disseminated in other print or electronic media by ITF, or entities with which it partners and any subsidiaries or partners thereof ("Affiliates"), or those opinions concerning cryptocurrencies expressed as and during the course of a public appearance, are for informational purposes only. Reports are provided for assistance and are not intended to, and must not, be used as the sole basis for an investment decision. The User assumes the entire risk of any use made of this information.

Reports may include projections, forecasts and other predictive statements which represent ITFs or its Affiliates' assumptions and expectations in the light of currently available information. These projections and forecasts are based on industry trends, circumstances and factors which involve risks, variables and uncertainties. The actual performance of a company, project, token or currency represented in a Report may vary from those projected. The projections and forecasts described in any Report should be evaluated keeping in mind the fact that they:

- are based on estimates and assumptions;
- are subject to significant uncertainties and contingencies;
- will vary from actual results and such variations may increase over a period of time;
- are not scientifically proven to guarantee certain intended results;
- are not published as a warranty and do not carry any evidentiary value; and
- are not to be relied on in contractual, legal or tax advice

Prospective investors/traders and others are cautioned that any forward-looking statements are not predictions and may be subject to change without notice. Reports based on technical analysis ("TA") are focused on studying charts and movements of a given currency or token's price movement and/or trading volume. As such, a Report based on TA may not match with a Report on fundamental analysis. Though Reports are reviewed for any untrue statements of material facts or any false or misleading information, ITF does not represent that ANY REPORT is accurate or complete and again emphasizes that NO REPORT should be relied on in connection with a purchase, investment, commitment, or contract by anyone whatsoever. ITF does not guarantee the accuracy, adequacy, completeness or availability of any information in any Report and therefore CANNOT be held responsible for any errors or omissions or for the results obtained from the use of such information. ITF, its Affiliates and the officers, directors, and employees of either, including analysts/authors shall not be in any way responsible for any direct, indirect, special or consequential damages that may befall any person from any information contained in any Report nor do they guarantee or assume liability for any omission of information from therein. Information contained in any Report cannot be the basis for any claim, demand or cause of action. These data, Reports, and information do not constitute scientific publications and do not carry any evidentiary value whatsoever.

# Disclaimers Continued

ITF's Reports are proprietary and are not for public distribution. Reproduction or dissemination, directly or indirectly, of research data and/or ITF Reports, in any form, is prohibited except with the written permission of ITF. Persons into whose possession the Reports may come are required to observe these restrictions. Opinions expressed therein are current as of the date appearing on the report only. Data may be subject to update and correction without notice. While ITF endeavors to update (on a reasonable basis) the information discussed in the Reports, there may be regulatory, compliance, or other reasons that prevent ITF from doing so.
The Reports do not take into account the particular investment objectives, financial situations, risk profile or needs of any person, natural or otherwise. The User assumes the entire risk of any use made of this information. Each recipient of a Report should make such investigation as deemed necessary to arrive at an independent evaluation of an acquisition of the asset referred to in any Report (including the merits and risks involved).

Cryptocurrencies involve substantial risks and are not suitable for all investors/traders. Investors can lose their entire investment relatively easily in the cryptocurrency markets. Before acting on any advice or recommendation in this material, Users should consider whether it is suitable for their particular circumstances and, if necessary, seek professional advice. The price and value of investments referred to in research reports and the income from them may fluctuate.

Certain information set forth in this Report contains "forward-looking information", including "future oriented financial information" and "financial outlook", under potentially applicable securities laws (collectively referred to herein as "Forward-Looking Statements"). Except for statements of historical fact, information contained herein constitutes Forward-Looking Statements and includes, but is not limited to, the (i) projected financial performance of a company, project, token, or currency; (ii) completion of, and the use of proceeds from, the sale of tokens being offered to the public; (iii) the expected development of a company, project, token, or currency's business, projects and joint ventures; (iv) execution of the company's or the project, token, or currency's developers' vision and growth strategy; (v) sources and availability of funding for the company, project, token, or currency; (vi) completion of any projects that are currently underway, in development or otherwise under consideration; (vi) renewal of any material agreements; and (vii) future liquidity, working capital, and capital requirements. Forward-Looking Statements are provided to allow potential investors the opportunity to understand ITF's beliefs and opinions in respect to the future of a given company, project, token, or currency so that they may use such beliefs and opinions as one factor in evaluating an investment.

NO statement issued on ITF's website or in any Report is a guarantee of future performance and undue reliance should not be placed on them. Such Forward-Looking Statements necessarily involve known and unknown risks and uncertainties, which may cause actual performance and financial results in future periods to differ materially from any projections of future performance or result expressed or implied by such forward-looking statements.

Although Forward-Looking Statements contained in this presentation are based upon what ITF and/or its Affiliates believe are reasonable assumptions, there can be no assurance that Forward-Looking Statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. Neither ITF nor any of its Affiliates undertake any obligation to update forward-looking statements if circumstances or management's estimates or opinions should change except as required by applicable laws. The User is cautioned not to place undue reliance on forward-looking statements.

The User should consult their own advisors to determine the merits and risks of ANY investment.