# Scalable Decentralized Systems : A Survey

Soheil Zibakhsh : University of Tehran, Iran

November 30, 2021

## Abstract

In recent years, Blockchain-based decentralized systems, more notably crypto-currencies, have drawn much attention from academia and industry. Many good properties explain Blockchain-based decentralization's success, like trust-free security, transparency, anonymity, and democracy. Despite these positive features, some obstacles keep these systems from reaching their full potential, more notably, the problems with scalability. This article focuses on the scalability issue and provides a brief survey on the recent research on the topic. We will describe the problem and some of the best attempts to try to tackle it.

## 1 Introduction

Blockchain as a distributed, incorruptible, and transparent database has attracted much attention amongst academia and industry. This system can provide trust-free security and complete decentralization without a need for a trusted third party. It provides transparency and anonymity in such a way that all the transactions and data are publicly available, yet the source is anonymous. These features have proved promising for Cryptocurrencies, Internet-of-Things, and edge computing [26][28][41].

An inherent problem with using a blockchain as a shared ledger is that it sacrifices scalability; Because all miners, currently 13.000 miners for Bitcoin, need to exchange, store, and verify every transaction in the system, the network limitations come into play[30]. Bitcoin is a good example to show some of the problems most Blockchains based shared ledges face. Blocks get mined at regular intervals (approximately every 10 minutes for Bitcoin), and each block has a limited size; this means that currently, the throughput of transactions is limited, Bitcoin is about 4.6 transactions per second, which is not nearly good enough compared with centralized systems like Visa, WeChatPay, and PayPal[1]; making it impractical to use blockchain based transactions, in everyday use cases. Furthermore, The Bitcoin consensus requires users to wait for other blocks to extend the block with our transactions in them to make sure that double-spending attack doesn't happen. Currently, the standard waiting time for a block to be confirmed is six blocks, which is roughly 1 hour [17]. Recently, users have been feeling the capacity limitations of Bitcoin through increased transaction fees and latency [11].

With an increasing demand for making transactions, users need to pay more transaction fees to make sure that their transaction is more profitable for a miner to make it into a block. Also, Queuing of transactions and network bandwidth will lead to a longer delay time until a transaction gets decided.

There already exist surveys on the subject [44, 40, 4, 42]. In this survey, we agree with [44]'s Taxonomy and most of the discussed solutions and will follow them in the following sections.

## 2 Taxonomy of Solutions

There have been many different ideas on how to solve this problem. Most of the proposals fall into three categories: $layer0$, $layer1$, and $layer2$ solutions. $Layer0$ solutions try to enhance the infrastructure, like the network that connects the nodes. $Layer1$ solutions try to enhance the blockchain's shortcomings by changing the consensus and protocols. $Layer2$ solutions propose ways to move away from the blockchain, and for this reason, they are also called off-chain solutions.

## 2.1 Layer2 Solutions

In layer2 solutions, the idea is to move transactions off-chain and effectively increase the throughput. Some promising proposals are the use of payment channels and side-chains.

### 2.1.1 Payment Channels

A Payment channel is a temporary off-chain trading mechanism in which users freeze some initial balance on the blockchain and can start to send each other credits with negligible cost. It is important to note that the amount of credit sent cannot exceed the chain's initial balance.

While having transactions with parties you have channels with is great, it is not a good idea to make a dedicated channel with every node in the system. Most payments in the system are not periodic, and instead of putting a payment channel contract on the blockchain, users can just make the intended transaction on the blockchain. To fix this problem, users can use networks of payment channels to transfer funds. Payment channels allow us to create a network of channels to send each other funds without having a direct payment channel. Nodes can pay a small routing fee to other nodes to route their payments. Bitcoin Lightning Network [30] and Ethereum Raiden network [27] are implementations of this proposal in practice.

This approach has proved promising in the past few years, and they raised some interesting research questions. Some of the main areas of focus have been network construction [6], network performance [7][6][14], routing [9][1], and privacy [16][36].

### 2.1.2 Side Chains

The main idea in Side Chains is to distribute transactions between different chains. The main challenge with this idea is blockchain interoperability, which remains an open area for research [31]. A direction taken to reach interoperability is to use Relays. The Cosmos network and Polkadot [22, 39] are implementations of connecting independent blockchains in a network.

Pegged Sidechain is one of the first proposals that enables Bitcoin and other blockchain-based cryptocurrencies to be transferred between different blockchains[2]. Another proposal is the Plasma smart contracts which essentially make a new chain with the root being in the main blockchain [29]; the idea is to have local parties create chains of their own, but the chain gets validated by the main Ethereum chain periodically.

Rollups are methods in which the computation and part of the data are transferred to the second layer and the second layer provides proofs of the transaction to the first layer. There are two types of rollups: optimistic-rollups and ZK-rollups[13]. Optimistic rollups use fraud proofs, while ZK-rollups use validity proofs. Moving tokens with both types of rollups are slow and expensive[38].

Commit-Chains [18] try to fix some of the problems with off-chain P2P solutions by using a centralized but untrusted third party as the payment gatherer to scale off-chain payments. Some interesting security questions like the possibility of DOS attacks and Anonymity will arise from this approach that requires solving. Nevertheless, this proposal shows promising experiment results in scaling to 1 billion users with relatively low transaction fees.

## 2.2 Layer1 Solutions

In layer1 solutions, the main focus is to increase the blockchain's throughput by fine-tuning some block parameters, like size, or by changing the entire protocol. We can separate the layer1 solutions into four categories: Block data, Consensus, Sharing, and DAG[44].

### 2.2.1 Block data

Increasing the blocksize increases the throughput because more transactions can fit in a block. Likewise, increasing the block generation rate will lead to more throughput. However, increasing the block size or block generation rate means that the blocks do not propagate through the network as effectively and quickly; moreover, bigger blocks need more time to evaluate. This causes numerous security problems, like the fact that an adversary needs less computational power(in PoW systems) to fork the blockchain and double-spend funds effectively; moreover, increasing the blocksize is not a sustainable solution to the scalability problem because we can't keep increasing the blocksize to infinity. Device capacity and network infrastructure will become our bottlenecks

again. With all that said, there have been some attempts to fine-tune the blocksize. Bitcoin Cash [15] is a hard fork on bitcoin that increased the blocksize from the initial 1 MB to 8 MB, which later increased further to 32 Mb.

Another approach is to increase the number of transactions a block can have instead of increasing blocksize. Segregated Witness (SegWit) is a type of contract that separates the signatures from the transactions, thus increasing the number of transactions that fit in a block. Also, Various block compression skims have been suggested to make use of the blocksize we already have [10].

### 2.2.2 Consensus

Decentralized systems need consensus. In 2008, Nakamoto[26] proposed a consensus for Bitcoin, which uses Proof of Work (PoW). In PoW consensus, Miners(the nodes suggesting blocks) need to solve a hard mathematical problem to get permission from other miners to suggest the next block. PoW is a novel consensus that many different blockchains have adopted. The difficulty of the mathematical problem is set in a way that it will take about 10 mins for someone in the network to find a solution(in the previous section, we discussed the problem with increasing the block generation rate). The PoW consensus suffers from long wait times and high energy wastes. The long wait period (approximately 1 hr) ensures that the transaction is at least six blocks deep in the chain, so it can't be double-spent. While some research has been done to improve the current PoW, like Bitcoin-NG[12], GHOST[33], and SPECTRE[32], many researchers have been looking towards other promising consensus algorithms like PoS and BFT.

Proof of Stake (PoS) avoids the computational overhead and gives the people with more stake in the blockchain a higher chance of being the next block proposer. This proposal has the risk of making the rich richer in a fashion that makes the system vulnerable. Some secure PoS have been proposed, like Ourobros[19], Ourobros praos[8], and Snow White[3].

In Delegated Proof of Stake[23], nodes holding tokens vote on one or a subset of nodes responsible for creating blocks. These solutions greatly increase throughput, but their decentralization might be in question.

Practical Byzantine Fault Tolerance (PBFT) works without computational overhead, but there is more communication overhead. A node is selected to take votes from other nodes In each phase, based on Byzantine Fault Tolerance. Tendermint[5] and Elastico[25] are proposals that use PBFT.

Hybrid consensuses are proposals that use the combination of the above ideas. For example ByzCoin [20] combines the ideas of PoW and PBFT.

### 2.2.3 Sharding

Sharding is a well-known method, first used in traditional database systems. The idea of sharding is to distribute the data to different fragments, to reduce the load from the main storage system. Applying the sharding technology to a blockchain is to divide the blockchain network into several smaller networks called shards. Each shard contains part of the nodes, and arriving transactions are divided amongst different shards; thus, each node needs to process a fraction of the transactions, and transactions can be processed in parallel. This can reduce the verification time and increase throughput. While sharding increases transaction throughput, there are some challenges like 1- how to reach a consensus between nodes of each shard (we have talked about possible consensus algorithms in the previous section), 2- to make sure attacks like double spending can't happen, 3- how to handle cross-shard transactions, 4- how to distribute nodes and transactions in each shard.

Elastico[25] uses PoW to elect committees of nodes per shard. The committee then uses PBFT to reach a decision, but it lacks cross-shard atomicity. Omniledger[21] solves some of Elastico's problems, like atomicity. RapidChain[43], Monoxide[37], Zilliqa[35], and Harmony are other implementations of sharding in blockchain, all with different properties.

### 2.2.4 DAG

In traditional blockchains, we store blocks of data on a single chain structure. The idea is to store the blocks in a DAG (Directed Acyclic Graph). By doing this, each block can have a pointer to more than one block. In this idea, blocks can be generated concurrently. Thus increasing the throughput of the blockchain. Some projects using DAG are Inclusive[24], SPECTRE[32], Phantom[34], Conflux, IOTA, Byteball, and Nano[24].

# 3 Conclusion

In this survey, we highlighted the issue of blockchain's scalability and several proposals on how to solve this problem. While most of the mentioned proposals solve the problem to some extent, there still exists a large research space to be explored and a lot of place for improvement. If we are to make blockchain one of the day-to-day technologies we use, we need to improve the mentioned proposals or develop novel solutions to solve the blockchain scalability problem.

# References


[1] Z. Avarikioti, L. Heimbach, Y. Wang, and R. Wattenhofer. Ride the lightning: The game theory of payment channels. In *International Conference on Financial Cryptography and Data Security*, pages 264–283. Springer, 2020.

[2] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. Enabling blockchain innovations with pegged sidechains. *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, 72, 2014.

[3] I. Bentov, R. Pass, and E. Shi. Snow white: Provably secure proofs of stake. *IACR Cryptol. ePrint Arch.*, 2016(919), 2016.

[4] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W.-C. Hong. A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access*, 8:54371–54401, 2020.

[5] E. Buchman. *Tendermint: Byzantine fault tolerance in the age of blockchains.* PhD thesis, 2016.

[6] M. Conoscenti, A. Vetrò, and J. C. De Martin. Hubs, rebalancing and service providers in the lightning network. *Ieee Access*, 7:132828–132840, 2019.

[7] M. Conoscenti, A. Vetrò, J. C. De Martin, and F. Spini. The cloth simulator for htlc payment networks with introductory lightning network performance results. *Information*, 9(9):223, 2018.

[8] B. David, P. Gaži, A. Kiayias, and A. Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 66–98. Springer, 2018.

[9] G. Di Stasi, S. Avallone, R. Canonico, and G. Ventre. Routing payments on the lightning network. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1161–1170. IEEE, 2018.

[10] D. Ding, X. Jiang, J. Wang, H. Wang, X. Zhang, and Y. Sun. Txilm: Lossy block compression with salted short hashing. *arXiv preprint arXiv:1906.06500*, 2019.

[11] D. Easley, M. O'Hara, and S. Basu. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134(1):91–109, 2019.

[12] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*, pages 45–59, 2016.

[13] A. Gluchowski. Zk rollup: scaling with zero-knowledge proofs. *Matter Labs*, 2019.

[14] Y. Guo, J. Tong, and C. Feng. A measurement study of bitcoin lightning network. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 202–211. IEEE, 2019.

[15] M. A. Javarone and C. S. Wright. From bitcoin to bitcoin cash: a network analysis. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pages 77–81, 2018.

[16] G. Kappos, H. Yousaf, A. Piotrowska, S. Kanjalkar, S. Delgado-Segura, A. Miller, and S. Meiklejohn. An empirical analysis of privacy in the lightning network. In *International Conference on Financial Cryptography and Data Security*, pages 167–186. Springer, 2021.

[17] G. O. Karame, E. Androulaki, and S. Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 906–917, 2012.

[18] R. Khalil, A. Zamyatin, G. Felley, P. Moreno-Sanchez, and A. Gervais. Commit-chains: Secure, scalable off-chain payments. *Cryptology ePrint Archive, Report 2018/642*, 2018.

[19] A. Kiayias, A. Russell, B. David, and R. Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference*, pages 357–388. Springer, 2017.

[20] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford. Enhancing bitcoin security and performance with strong consistency via collective signing. In *25th {usenix} security symposium ({usenix} security 16)*, pages 279–296, 2016.

[21] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford. Omniledger: A secure, scale-out, decentralized ledger via sharding. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 583–598. IEEE, 2018.

[22] J. Kwon and E. Buchman. Cosmos whitepaper, 2019.

[23] D. Larimer. Delegated proof-of-stake (dpos). *Bitshare whitepaper*, 81:85, 2014.

[24] Y. Lewenberg, Y. Sompolinsky, and A. Zohar. Inclusive block chain protocols. In *International Conference on Financial Cryptography and Data Security*, pages 528–547. Springer, 2015.

[25] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena. A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 17–30, 2016.

[26] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[27] R. Network. What is the raiden network, 2019.

[28] O. Novo. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5(2):1184–1195, 2018.

[29] J. Poon and V. Buterin. Plasma: Scalable autonomous smart contracts. *White paper*, pages 1–47, 2017.

[30] J. Poon and T. Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.

[31] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski. Towards blockchain interoperability. In *International conference on business process management*, pages 3–10. Springer, 2019.

[32] Y. Sompolinsky, Y. Lewenberg, and A. Zohar. Spectre: a fast and scalable cryptocurrency protocol. *IACR Cryptol. ePrint Arch.*, 2016(1159), 2016.

[33] Y. Sompolinsky and A. Zohar. Secure high-rate transaction processing in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 507–527. Springer, 2015.

[34] Y. Sompolinsky and A. Zohar. Phantom. *IACR Cryptology ePrint Archive, Report 2018/104*, 2018.

[35] Z. Team et al. The zilliqa technical whitepaper. *Retrieved Sept*, 16:2019, 2017.

[36] S. Tikhomirov, P. Moreno-Sanchez, and M. Maffei. A quantitative analysis of security, anonymity and scalability for the lightning network. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 387–396. IEEE, 2020.

[37] J. Wang and H. Wang. Monoxide: Scale out blockchains with asynchronous consensus zones. In *16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19)*, pages 95–112, 2019.

[38] C. Whinfrey. Hop: Send tokens across rollups. 2021.

[39] G. Wood. Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper*, 21, 2016.

[40] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu. A survey on the scalability of blockchain systems. *IEEE Network*, 33(5):166–173, 2019.

[41] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang. Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(2):1508–1532, 2019.

[42] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu. Survey: Sharding in blockchains. *IEEE Access*, 8:14155–14181, 2020.

[43] M. Zamani, M. Movahedi, and M. Raykova. Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 931–948, 2018.

[44] Q. Zhou, H. Huang, Z. Zheng, and J. Bian. Solutions to scalability of blockchain: A survey. *IEEE Access*, 8:16440–16455, 2020.