Scalability Options for Blockchain Technology

Robin Huwa

Lehrstuhl für Technische Informatik der Universität Passau

Introduce what Blockchains are in General.

Abstract. Distributed blockchains have gained great notoriety in the past decade since their creation in the abstract in 2008 and their usage increased rapidly. Also the number of alternative Bitcoin-derivatives based on very similar blockchain technology exploded. Millions of users and gigawatts of computational energy per year are now involved in Bitcoin alone, nevertheless there are inherent design flaws that prohibit the necessary performance to compete with more traditional centralized systems. In this paper the possible solutions to improve blockchain scalability will be presented.

Keywords: Bitcoin · Scalability · Proof of Work · Byzantine Fault Tolerance · Blockchain · Lightning Network · EOS.IO · Bitcoin-NG

1 Introduction

Why is there a need to improve scalability in distributed blockchains?

As of May 2018, there are close to 25 million Bitcoin wallets for about as many users and and the popular blockchain has enjoyed a superlinear growth of users, especially since 2014 [1]. There does not seem to be a deceleration of this growth coming in the near future, and as the numbers grow, the demands on the system rise as well since more and more transactions are taking place. The current Bitcoin system has a maximal throughput of seven transactions per second [10]. In contrast, more centralized transaction systems like credit card institutes (Visa) may reach up to 56,000 transactions in a single second [3], which is orders of magnitude higher than what Bitcoin can potentially offer in the current state of affairs. Additionally, the actual empirical throughput is less than half of that if all involved latencies are totalled [5].

Why

To discuss the options put forward to remedy this deficiency, various technical terms need to be explained. The main focus of decentralized systems like Bitcoin is the *Blockchain*, a virtual ledger which is replicated on every contributing node, containing all previous transactions in total order split up into blocks. A *Block* has a uniquely defined hash value representative of its predecessor in the ledger, and contains an again totally ordered set of transactions. One of the factors of performance in such a distributed system is *Block Size*, the actual data size of one block. Another one is *Block Frequency*, the mean time it takes to compute (*"mine"*) a block. In Bitcoin today, the block size is set to 1MB and the block frequency comes to 10 minutes [10].

Architecture Sketch for Understandability

The whole *mining* process can be seen as an inherent aspect of the Proof of Work protocol. Nodes have to spend computational resources and electrical energy when they are mining a block to disincentivize adversarial nodes from flooding the system with invalid blocks, as only valid blocks are remunerated [2]. In Bitcoin, the proof of their work is a computed hash value that has to be smaller than a certain threshold, which is dynamically adjusted as the system operates to secure that these correct hash values are only found in intervals in length of the block frequency [10]. It is suspected that finding these correct hash values is a NP-hard problem, as so far nodes have to brute force search for them, but the verification by other nodes is very quick. All in all, this process needs to be accelerated massively to allow a realistic, scalable use of the system in the future.

Isn't Mining limited? (Difficulty) Why faster? -> the faster it will be the "less" value you can mine.

This document is structured as follows. The different possibilities of improving scalability are described in Section 2. Subsection 2.1 deals with optimizing the current Proof of Work system, of which the operating principles will be outlined, while in Subsection 2.2 the byzantine fault-tolerant approach for decentralized consensus will be defined and further discussed. In sections 3 and 4, Bitcoin-NG and EOS.IO, two new technologies that differ from the original concept of Bitcoin by implementing protocols varying from traditional Proof of Work, are introduced and their techniques outlined. Section 5 summarizes this report and gives an outlook on the most probable options that will be chosen to change cryptocurrencies like Bitcoin in the near future.

2 Overview of Scalability Improvements for Blockchains

There are possibilities to improve the blockchain's performance without having to replace the Proof of Work protocol completely, which will be discussed in the subsequent section. But first, the simpler solutions that work within the present system are introduced.

What is "Proof of Work" Protocol. => Explain.

2.1 Optimizing current Proof of Work design

The most basic changes start with the existing parameters like block size and block frequency but those are by far not the only options presented that will speed up the system, and at the end a method to utilize the blockchain framework to support off-chain transactions will be explained. The main advantage of these solutions is that they allow the existing system to continue operating, whereas a completely new implementation would effectively need to bootstrap itself from the very beginning.

Fine Tuning the current parameters The block size and block frequency parameters have their own upper or lower bounds that are dependent on the underlying system, as physical delays cannot be ignored when considering the best practical solution.
Reducing the block frequency will increase the throughput of transactions, but

it should not be lowered past twelve seconds, as this constitutes the general network delay between nodes [3]. When blocks are created faster than the network delay, they have to be queued for receiving nodes and those are effectively disabled from mining on top of the most recent block, as they do not receive it on time.
Similarly, the block size has to adhere to an upper bound for practicality. A greatly increased block size would offer more transactions per block and therefore less overhead, but due to the meager median bandwidth between the interconnected nodes the propagation of blocks would take up much time. After reaching a certain threshold in block size, more and more weaker nodes with low bandwidth are unable to receive a block quickly enough before the following block is already mined by other, stronger nodes. Again, these weaker nodes and their processing power would effectively be excluded from mining blocks, reducing the overall computational power of the system and centralizing it further towards the stronger nodes, contrary to the original idea of a blockchain. In Bitcoin, this practicality threshold lies at about 4Mb for the block size, as most nodes are able to receive those on time within the current 10min block frequency [3].

Views for the Blockchain The term *View* comes from database technology, in which it describes a virtual read-only resource created from a set of data which is subjected to certain conditions. The view just consists of the resulting set of data computed from the original data with the given constraints.
Now in Bitcoin, active currently processed transactions spend amounts that depend on previous transactions' spending. A wallet's balance is counted as the total amount of funds from received transactions, and transactions from this wallet may only spend funds received from previous transactions.
So if an old transaction has already been referenced, it cannot be used again as a source for future transactions, therefore it is needless to include that transaction in any future validation. To more efficiently utilize a node's space, a type of view should be created that only displays non-referenced transactions, known as UTXO, the "unspent transactions output" [3, 9]. This also could greatly reduce the bootstrap time, which takes about four days in the current system, since the complete ledger has to be downloaded [3]. The blockchain size has seen a strong, superlinear increase and as of May 2018 it needs ∼168GB of space as all transactions from the beginning in 2009 are included.

Segregated Witness This proposal aims to fundamentally change the layout of the storage of a transaction, whereas data that is needed to determine a transactions' validity, such as signatures of the involved entities, is saved in this new substructure called the *Witness* [8]. Different to the preexisting approach, the content of this substructure is not part of the transaction's hash, which is used to reference it in future transactions as described in the paragraph "Views for the Blockchain". This is solved as such because the witness data is only needed for validation, and when validation is not required the witness data does not need to be transmitted, therefore the exclusion of this data will not change the

transactions' hash in this adapted hashing method. This explains the *Segregated* part of the title. Following that, the witness' size is not evaluated for the transaction's total size which allows a block to contain more transactions, therefore increasing the throughput of the system without increasing the raw data as much as simply increasing the block size [8].
Although this upgrade might quadruple the throughput in certain optimal cases [6], this won't come close to resolving the scalability problem. More importantly, Segregated Witness eliminates transaction malleability consequences, in which it is possible to slightly alter signature data of a transaction while it is not yet confirmed, which leads to a different hash identifier for the transaction while the actual contents of the transaction have not changed [8]. This is of course problematic for other transactions referencing the "malleabled" one and prohibited technologies like the Lightning Network that actually might remediate the scalability problem, which will be described in the following paragraph. After all, Segregated Witness is already implemented in the Bitcoin protocol, but only a minority of users are interested in adopting the change as of yet.

Off-Chain Payment Channels The blockchain system implements an immutable, persistent ledger. As it is also replicated on every participating node it is a secure protocol for transactions between entities, but this comes at a cost. Every transaction encoded in a block that is saved on the blockchain needs electrical energy for all the inter-node communication and more crucial, the mining process that uses a lot of computational resources. This has to be remunerated accordingly, which takes shape in fees that are charged per transaction, which make micro-transactions with very small values impractical. Adding to that, if it was possible to decrease the total number of noted transactions of the ledger the whole system could be sped up. To support "compressed" transactions while retaining full blockchain functionality, the decentralized system must be used as a backbone. This falls into the abstract category of "Off-Chain Signature Pattern" [4], in which a pair of entities in the decentralized system minimalize the cost of already planned transactions (e.g. ongoing contracts) for their own monetary and the system's computational benefit.
To do so, two entities can create a one-sided channel that saves the total funds to be spent, and in a certain time frame micro-payments that are taken from those funds can be sent privately from the payer to the payee. Those micro-payments are not seen in the blockchain, only the channel transaction with the total transferred amount [4]. This can be further refined into bidirectional communication, as does the Lightning Network.
The *Lightning Network* by Poon and Dryja [9] aims to radically reduce the number of transactions that the blockchain has to process. Originally designed to improve privacy, this technology changes the nature of previously uniform transactions, of which every single one has to be seen by all (or at least most) nodes in the system. These are now split into two categories: *Public* transactions that are appended onto the ledger, and *private* transactions that are only seen by the participating parties. When two parties enter into a continuous business

relationship where multiple transactions happen between themselves, there is no need to note each transaction in the blockchain as long as both parties agree on the outcome. Only at the very end of the relationship do the parties send a final transaction to the public blockchain to disclose the conclusion of their contract with their respective balances. The improved privacy implications of this alteration are clear as less information is published on the blockchain but instead is tunneled through a private channel, but more importantly in this context the total amount of transactions processed by the system is decimated in certain cases.
In the Lightning Network this procedure starts with a public *Funding Transaction*, signed by both participants, which locks their funds so they cannot use those funds in other transactions as long as contract is open [9]. This initial transaction also marks the start of the implied channel through which the private transactions follow up. Those are called *Commitment Transactions* and change the balances of the locked funds, also those have to be signed by both participants to express their agreement with the change [9]. These are *not* published to the blockchain. When the participants want to close the channel and publish their monetary exchange to the blockchain, the very last commitment transaction can be broadcast to the other nodes and the output is now a persistent, official part of their respective Bitcoin accounts.
As this proposal has undergone long development and many proponents are convinced of its benefits, this might be a probable long-term solution for Bitcoin's scalability problem without changing the system radically. But there are different approaches that have more rigorous changes to allow for better scalability, which are presented in the following sections.

2.2 Byzantine Fault-Tolerant Approach

what is the failure that is induced?

A Byzantine Fault-Tolerant system is a replicated state machine that can fully function when less than one third of all nodes are byzantine (or not honest) actors [10]. In blockchain fabric, that means if more than two thirds of all nodes agree on a ledger state the system is working correctly. After a certain scale the system is very hard to attack for individual or small groups of nodes willing to abuse the system, and there is no inherent need for limitless continuous computations as experienced in the Proof of Work protocol.
The main disadvantage is the need for each node to know all other nodes, to know if sufficient consensus is achieved [10]. Because of that, these BFT protocols depend on a comparatively static environment to function, which has excluded them from any implementation for a completely decentralized, uncontrolled blockchain. As there is development to adapt existing BFT protocols for wide-spread use, this might overtake all existing blockchains as BFT approaches generally allow for a much faster system. But as of today there is not much to report on, we have to wait what future work will offer.

3 Bitcoin-NG - Best of both Worlds?

Bitcoin Next Generation is the full name of the Bitcoin-NG protocol devised by I. Eyal, A. E. Gencer, E. G. Sirer and R. van Renesse [5]. It is build upon the traditional concept of the distributed ledger, the blockchain, although with now two different types of blocks: keyblocks and microblocks.

Also here a small graph would be beneficial for understanding

Keyblocks are comparable in creation to the blocks of the original Proof of Work protocol, as every miner tries to find a correct nonce value needed to receive a cryptographic hash of the keyblock under a certain dynamically adjusted target. But these keyblocks only include the public key of the node that mined it, which becomes the current leader. Due to the minimal information contained in the keyblock, lacking any transactions, it is rapidly distributed in the decentralized system, which decreases the chance of concurrent leaders and therefore forks. The current leader is the only one allowed to append transactions to the blockchain, those are packaged into microblocks that are not mined, but simply signed by the leader. Therefore the entry of transactions into the ledger happens almost as fast as the network permits, whereas other nodes are mining new keyblocks. When another node becomes the leader, its new keyblock's validity can be verified quickly due to the inherent nature of the Proof of Work protocol and the transition from the previous leader to the new one is smooth and does not induce any significant latencies between epochs, as the timeframes for distinct leaders are called. Microblocks signed by the correct current leader that are received by a node are simply added to their local ledger copy and distributed to other nodes, without the need to verify the hash value of the block but only the leader signature, which reduces distribution delay further.

When comparing this improved protocol to the original Bitcoin protocol, the striking distinction is the different view on the timeline of transactions compared to the blocks they are included in: In Bitcoin, transactions happen and then are gathered into a block that needs to be mined before it is included in the blockchain. In Bitcoin-NG, the leader mines a keyblock to achieve his position and all happening transactions can be collected into a quickly deployed microblock and pushed onto the blockchain without the high Proof of Work computation delay. This is the reason why Bitcoin-NG can function at orders of magnitude higher throughput rates than traditional blockchain protocols.

The first cryptocurrency to successfully implement this new protocol is *Waves-NG*, a revamp of the previous *Waves* Bitcoin-derivative now using this new system. While it has not come to fame, is is build on a more future-proof system and may outlast other competitors in the long run. It can be found under https://waves-ng.wavesplatform.com.

4 EOS.IO - Democracy in Blockchain Fabric

be precise; year etc...

EOS.IO is a fairly new software that aims to be a coherent distributed system not only as a cryptocurrency, but also for many different decentralized applications such as parallel computing or authentication without the need for a trusted

intermediary, instead building up on top of the trustless concept of the original Bitcoin implementation. But on the contrary, it does not rely on any Proof of Work computation of nodes eager to add blocks onto the virtual ledger. Contributing nodes, called producers, are elected by users of this cryptocurrency and the former are allowed to create blocks in a certain time slot, which is partially defined by the blockchain as it is split into small time intervals [7]. The other factor is the total number of nodes appending to the ledger, since every single one of those has its own timeslot to create a block, which will also be signed by all other producers. After the producers have signed the blocks they altogether have created, the votes will be reevaluated and the producers might change depending on a differential vote outcome, as the total number of producers is limited. This algorithm is known as Delegated Proof of Stake.
Delegated Proof of Stake is different from other proposed algorithms in that it is deterministic, not just highly probabilistic like Bitcoin's Proof of Work. In Bitcoin, a block (and therefore a transaction in this block) is *not* considered confirmed right after it has been added to the blockchain, since forks are still possible even when the blocks are produced in ∼10 minutes intervals, which is only that long to reduce fork development to a manageable level. Instead, a block is considered confirmed when other new blocks are mined on top of the original. After a certain amount of blocks the probability that a fork exists with more blocks but with a different starting point is so insignificant that the block is for all intents and purposes an immutable part of the blockchain. In Bitcoin, a block is considered practically confirmed after about one hour, an inacceptable amount for any serious transaction system [10].
In Delegated Proof of Stake however, nodes are not competing for their own blocks to be included as in Bitcoin, but they are working together, each creating one block in their own predefined time slot and signing other blocks. Once a block has more than two thirds of all producers' signatures, it is considered confirmed and a persistent part of the blockchain. That means in EOS.IO with its half a second block interval, consensus is achieved within a mere second [7], which is better than any traditional protocol can offer.

5 Conclusion

are there also other application areas than "money"?

In summary, there are many options for Bitcoin and its alternatives to consider when deciding on improvements, and only the more probable and interesting ones have been presented in this document. Whereas small changes to preexisting factors like block size can offer some leeway for the near future, a new protocol has to be devised to make any of these blockchains fundamentally scalable. After almost a decade of Bitcoin reigning supreme, its inherent issues have to be addressed. EOS.IO offers an interesting divergence for that exact reason, and without a doubt there are many more future-oriented protocols on their way to remediate whichever problem the respective designers think of as the most striking.

References

1. Blockchain wallet users (2018), https://blockchain.info/charts/my-wallet-n-users?timespan=all
2. Ammous, S.H.: Blockchain technology: What is it good for? Available at SSRN: https://ssrn.com/abstract=2832751 (2016)
3. Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Gün Sirer, E., Song, D., Wattenhofer, R.: On scaling decentralized blockchains. In: Clark, J., Meiklejohn, S., Ryan, P.Y., Wallach, D., Brenner, M., Rohloff, K. (eds.) Financial Cryptography and Data Security. pp. 106–125. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
4. Eberhardt, J., Tai, S.: On or off the blockchain? insights on off-chaining computation and data. In: De Paoli, F., Schulte, S., Broch Johnsen, E. (eds.) Service-Oriented and Cloud Computing. pp. 3–15. Springer International Publishing, Cham (2017)
5. Eyal, I., Gencer, A.E., Sirer, E.G., Renesse, R.V.: Bitcoin-ng: A scalable blockchain protocol. In: 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). pp. 45–59. USENIX Association, Santa Clara, CA (2016), https://www.usenix.org/conference/nsdi16/technical-sessions/presentation/eyal
6. Herrera-Joancomartí, J., Pérez-Solà, C.: Privacy in bitcoin transactions: New challenges from blockchain scalability solutions. In: Torra, V., Narukawa, Y., Navarro-Arribas, G., Yañez, C. (eds.) Modeling Decisions for Artificial Intelligence. pp. 26–44. Springer International Publishing, Cham (2016)
7. Lee, G., Cox, T., Prioriello, W., Ma, Q., Lavin, J., Larimer, D., Hourt, N., 'testz': Eos.io technical white paper v2 (2018), https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
8. Lombrozo, E., Lau, J., Wiulle, P.: Bip 141: Segregated witness (consensus layer) (2015), https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki
9. Poon, J., Dryja, T.: The bitcoin lightning network: Scalable off-chain instant payments (2016), http://lightning.network/lightning-network-paper.pdf
10. Vukolić, M.: The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In: Camenisch, J., Kesdoğan, D. (eds.) Open Problems in Network Security. pp. 112–125. Springer International Publishing, Cham (2016)