Analysis of the possibilities for improvement of BlockChain technology

Daniela Mechkaroska, Vesna Dimitrova and Aleksandra Popovska-Mitrovikj

***Abstract* — *Bitcoin* and *Smart Contract* are the first major applications of the BlockChain technology. But, with increasing the number of transactions, the process of verification on every transaction is very slow. This is the reason for a third major innovation called a BlockChain scaling. The scalability is a process of taking certain steps in accelerating the performing of transactions in this new technology.**

In this paper we analyze the possibilities for BlockChain scalability and we examine the advantages and disadvantages of the proposed solutions.

***Keywords* — Bitcoin, BlockChain, cryptocurrency, double spending, scalability, SmartContact.**

I. INTRODUCTION

BITCOIN is a peer-to-peer version of the electronic cash and it is the first major application of BlockChain, for direct online payments from one party to another without the need of trusted third party. Transactions with this cryptocurrency are secured by cryptography. In order to become part of the bitcoin peer-to-peer network it is necessary to install the open source program that implements this new protocol [1].

Smart Contract is the other major application of BlockChain which is an agreement of exchanging a value or assets between two owners based on a set of conditions, which can agree between themselves through the BlockChain [2]. Some of their applications are described in [3].

Since the process of verification on every transaction is very slow, there is a need for a third major innovation called a BlockChain scaling. A scaled BlockChain makes the process faster by investigating:

- how many confirmations are necessary to validate each transaction and to separate the work efficiently and
- the limits on the amount of transactions the bitcoin network can process.

This modification does not sacrifice security of BlockChain. A scaled BlockChain is expected to be fast enough to power the Internet of things and go parallel with the major payment middlemen (for example: VISA and PayPal) of the banking world [4].

The rest of the paper is organized on the following way. In Section 2, we briefly describe the first major application of BlockChain technology, the crytocurrency called Bitcoin and explain the double spending problem. Analysis of several solutions for BlockChain scalability is given in Section 3. At the end, we give some conclusions for possibilities for improvement of BlockChain technology.

This research was partially supported by Faculty of Computer Science and Engineering at the University "Ss Cyril and Methodius" in Skopje

Daniela Mechkaroska, Vesna Dimitrova, Aleksandra Popovska-Mitrovikj are with the Faculty of Computer Science and Engineering, University "Ss Cyril and Methodius" - Skopje, P.O. Box 393, R. of Macedonia (phone: +389-71-277039;

e-mails:{daniela.mechkaroska, vesna.dimitrova, aleksandra.popovska.mitrovikj}@finki.ukim.mk.

II. BITCOIN AND THE DOUBLE SPENDING PROBLEM

A. Bitcoin

Bitcoin is a crytocurrency that has these three characteristics: decentralization, confidence and authentication.

Decentralized means non-existence of a central bank. Emitters of this currency are the users or holders of "mining" computers who verify the transactions.

Confidentiality is a property that information is not made available or disclosed to unauthorized entities. The confidence of this cryptocurrency is provided by public key cryptography.

Authentication is a process that ensures and confirms a user's identity. Authentication in the transactions from one to another peer in BlockChain network is made with digital signature. Digital signatures are ways that enable integrity, non-repudiation, and authentication in order to access the contens of networks data transaction.

Bitcoin miners verify the transactions, put them into blocks of transactions and decide which block is the next one, i.e., bitcoin system groups the transactions into blocks and connects them in BlockChain. This protocol in which miners "mine" cryptocurrency by solving crypto-puzzles is known as proof of work. Since, many people can create blocks at the same time, which block will enter first in BlockChain is decided by using a hash function.

A hash function is a function that takes as input a string of arbitrary length, performs an operation on it, and returns output data of a fixed length. In Bitcoin system hash function is used twice. Most often SHA-256 hashes are used and RIPEMD-160 hash is used for creating a shorter hash for a bitcoin address.

B. The double spending problem

As mentioned in the introduction, a scaled BlockChain makes the process faster without sacrificing security. In the mining process, a new block is made and included in a BlockChain approximately every 10 minutes. One transaction is confirmed when it is included in the block which is added to the BlockChain [5].

When the transaction is included in a block which is distributed in BlockChain network, that transaction is

978-1-5386-7171-9/18/$31.00 ©2018 IEEE

mined at depth of one block (one confirmation of the transaction). With each new block in the BlockChain, the depth of the existing blocks is increased by one. The transaction is verified when the block depth is at a specific level (six is a common number of confirmations) [6].

Double spending means using the same bitcoins more than once. Once a transaction is confirmed, it is impossible to double-spend it. The probability of a successful double spend is calculated according to Poisson distribution [7]:

$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-\left(\frac{q}{p}\right)^{z-k}\right)$$

where

- $\lambda = z\frac{q}{p}$ is the mean;
- z is the number of confirmations of transaction (the number of blocks by which the honest node has an advantage over the attacker);
- q is the attacker's percentage of Network Hash Rate (probability the attacker finds the next block);
- $p = 1 - q$ is probability an honest node finds the next block.

Table 1 and Fig. 1 presented the probability of a successful double spend given by a hash rate proportion and number of confirmations [8].

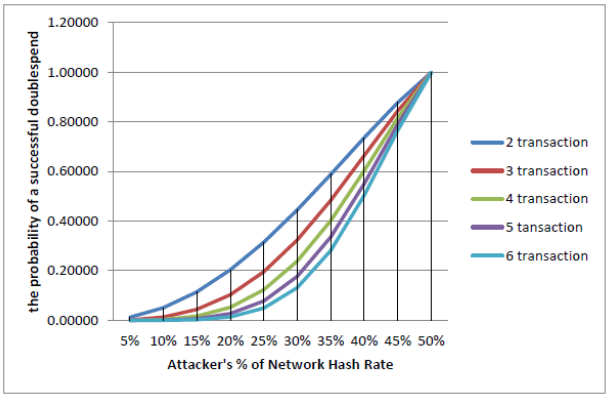

Fig. 1. The probability of a successful double spend

TABLE 1: ATTACKER SUCCESS PROBABILITY

Attacker's % of NHR	2 conf.	3 conf.	4 conf.	5 conf.	6 conf.
5 %	0.01265	0.00164	0.00022	0.00003	0.000004
10 %	0.05098	0.01317	0.00346	0.00091	0.00024
15 %	0.11504	0.04423	0.01725	0.00678	0.00268
20 %	0.20393	0.10324	0.05300	0.02742	0.01425
25 %	0.31544	0.19612	0.12351	0.07836	0.04994
30 %	0.44572	0.32458	0.23913	0.17735	0.13211
35 %	0.58881	0.48446	0.40251	0.33637	0.28217
40 %	0.73640	0.66417	0.60340	0.55063	0.50398
45 %	0.87772	0.84440	0.81561	0.78979	0.76611
50 %	1	1	1	1	1

The number 6 is chosen as an assumption that an attacker cannot possess more than 10% of the whole hash rate and the risk of 0.1% or less can be accepted [9]. But, for example, if the hash rate is around 40% then 90 confirmations are needed to have less than 0.1% chance for success of the attack (an attack for double spending of the transaction called "alternative history attack").

How does Bitcoin system handle the double spending problem?

We present an example to explain handling with double spending problem:

- Let A has one bitcoin and he want to send it to B. This transaction (called T1) goes to the pool of unconfirmed transactions and wait to be confirmed.
- At the same time A sends one bitcoin to C. This transaction (called T2) also goes into the pool and wait for confirmation.
- Let first transaction T1 is pulled out of the pool of unconfirmed transactions. Before the transaction is included into the BlockChain, its validity is checked. This transaction will be valid since A has one bitcoin and it is inserted into the BlockChain. Now, transaction T2 is pulled out of the pool, but it is invalid (since A has no more bitcoins) and will not be confirmed.
- If transactions T1 and T2 are validated simultaneously, then the BlockChain has two branches and the first one to reach the next block of confirmations will be confirmed.
- If T1 and T2 achieves the next block simultaneously, the race for the next block continue.
- Therefore it is recommended to wait 6 confirmations for completing transaction. As, we can see in Table 1, it is highly improbable that the transactions will reach the next block simultaneously more than 6 times. So, at the end only one transaction will be confirmed.

Alternative history attack is 100% probable to succeed if the attacker is in control of more than half of the network hash rate. The attacker can continue with his private fork until the moment it becomes longer than the branch built by the honest network because he can now generate blocks faster than the other participants of the network [10].

III. BLOCKCHAIN SCALING

Nakamoto introduced a block size limit of 1MB for every block in the public BlockChain. This was a security measure, so any block over that limit would be immediately rejected by the P2P network. This limitation slows down the transactions and cannot keep up with the speed of other currencies payment and credit cards.

In Table 2 is given a review of the average number of transactions made with cryptocurrencies and standard credit card [11]. Bitcoin has a limit of 3 to 4 transaction per second (although theoretically process up to 7, but that number is never being reached). This is not the situation with private BlockChain. They can reach over 1000 transactions per second, because each node on the network in private BlockChain uses high-quality computer with strong bandwidth internet connection.

TABLE 2: BITCOIN AND ETHEREUM VS VISA AND PAYPAL TRANSACTIONS PER SECOND

Currency	**Transaction per second**
Bitcoin	3 to 4 transactions per second
Etherium	20 transactions per second
PayPal	193 transactions per second average
Visa	1,667 transaction per second

There are several solutions for BlockChain scalability that have been or will be implemented. Some of the major ones are:

- Segwit
- Block Size Increase
- Sharding
- Proof of Stake.

Segwit or *segregated witness* is an alternative solution for BlockChain scalability, through increasing the number of transactions in a block, without increasing the size of the block. Segregated witness helps to enlarge the space for new transactions by removing signature data from bitcoin transactions. The proposal in segregated witness is to remove the digital signatures and store it outside the base transaction block. In this way "validating" part has been separated from the "effective" part of the transaction and more transactions can fit in a block without increasing the block size [12].

The digital signature takes 65 percent of transaction. If it is removed, more space will be free up in the bitcoin's block for more transactions. A new unit for transaction size is introduced by Segwit. Now, the transaction is divided in two parts: non-witness data (which must be stored on the block like before) and witness data (which is moved to the extended block). Non-witness data byte counts as 4 WU (weight units) each, while witness data byte only counts as 1 WU each. The maximum capacity of a block is 4 kWU, which would correspond to the old maximum block size of 1MB if no one uses Segwit. The Segwit upgrade to the Bitcoin protocol occurred in August 2017. A new format is used by around 30 percent of transactions [13].

According to BitMEX research the percentage of transaction that use SegWit is given on Fig 2.

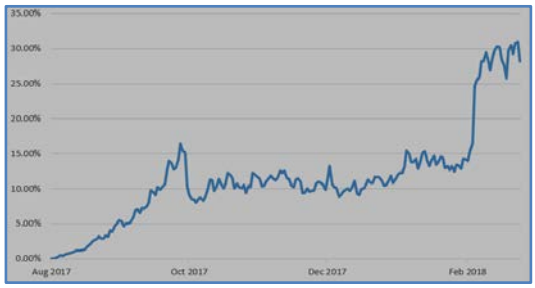

Fig. 2. Percentage of transactions that use SegWit [14]

Block Size Increase. In the bitcoin`s BlockChain the block size is limited to a maximum of 1MB. There are several arguments for and against increasing the size of blocks. A major argument against block size increase is that it will cause increased centralization.

Each connected computer on the bitcoin network is called a node. There are two types of nodes in bitcoin BlockChain: full nodes and lightweight (or partial) nodes.

Full nodes validate every block and transaction. Therefore, full nodes must store a copy of the complete BlockChain ledger locally (more than 165 GB).

The lightweight nodes do not store the complete ledger. They use a simplified payment verification (SPV) mode which only requires to download a copy of the block headers of the longest proof of work chain [7].

On the other hand, a miner creates blocks in the BlockChain that the nodes keep. Bitcoin network is maintained by roughly 10.000 full nodes, while the number of miners estimated to be around 100.000.

Increasing the block size makes the full nodes more expensive to operate. This leads to less hashers running full nodes and centralized entities would have more power, that weakens bitcoins value proposition. Miners have benefit from increasing of the block size, since increased block size means more transactions per block. This will increase the amount of transaction fees that a miner can make from mining a block.

Sharding. One of the biggest problem for cryptocurrencies is the speed of transaction verification. Each full node in the network has to store the entire BlockChain. Sharding breaks down a transaction into shards, spreads it among the network and nodes work on individual shards side-by-side. On this way, the overall time taken is decreased. A normal block has a block header and a body that contains all transactions in the block. The Merkle root of all transactions is in the block header. Sharding changes this into two levels of interaction.

The first level is the transaction group which is divided into a transaction group header and a body. Each shard has its own group of transactions. The transaction group header is divided in left and right part. The left part contains: Shard ID, Pre state root (state of the shard root before the transactions were applied), Post state root (state of the shard root after the transactions are applied) and Receipt root (receipt root after all the transactions in the shard are applied). The right part is full of randomly chosen validators who verify transactions in the shard. The transaction group body has the transaction`s IDs of all transactions in the shard.

The second level is the normal block chain, but here it contains two primary roots: the state root (represents the entire state which is broken down into shards) and the transaction group root (contains all transactions groups inside that block).

With Sharding many parallel transactions can happen at the same time and therefore the performances are increased. Each receipt of transaction can be easily accessed via multiple Merkle trees from the Merkle root of the transaction group. Also, the receipts are stored in a distributed shared memory that can be seen but not modified by other shards [15].

Zilliqa, a new BlockChain platform based on the technology of Sharding that solves the scalability issue faced by current BlockChain platforms like Bitcoin and Ethereum, has announced the release of their public test net. In Table 3 comparison of the capability of processing transactions in Ethereum and Zilliqa is given.

TABLE 3: COMPARISON OF CAPABILITY OF PROCESSING TRANSACTIONS IN ETHEREUM AND ZILLIQA

	Number of full nodes	Number of transactions per sec.
Ethereum	25000	15-20
Zilliqa	1800	1218

If the number of nodes in Zilliqa is double to 3600 the throughput scales as well to 2488 transactions per second [16] [17] [18].

From Table 3 it is clear that Zilliqa even with less number of nodes is able to process much more transactions per second than Ethereum or Bitcoin.

Proof of Stake. Most cryptocurrencies follow the proof of work protocol, which means that miners mine cryptocurrencies by solving crypto-puzzles using dedicated hardware. In proof of stake protocol there are validators instead of miners. The validator have to invest (lock up) some of his assets as stake. Then the validator starts validating blocks on the following way: if he sees a block that he thinks can be added to the BlockChain, he validates the block by putting a bet on it. If the block gets appended to the BlockChain, the validator will receive a reward proportional to the invested stake. If the validator bet a malicious block, the stake he has invested will be taken from him. Ethereum implement proof of stake protocol using the Casper consensus algorithm [15]. The advantage of using proof of stake protocol instead of proof of work is that it uses considerably less energy and as a result is more cost effective.

TABLE 4: COMPARISON OF PROOF OF WORK AND PROOF OF STAKE PROTOCOLS

	Proof of work	Proof of stake
Energy consumption	High	Low
Required tools	Mining equipment	No equipment necessary
Security	High	Untested
Decentralized vs. Centralized	Tends to centralize	Users can remain in control of their tokens

In Table 4 a comparison of some parameters of proof of stake and proof of work protocols is given [19].

IV. CONCLUSION

One of the biggest problems in BlockChain technology is the verification process that slows down the transactions. In this paper we analyze the possibilities for improvement of BlockChain without sacrificing security.

First we explained the double spending problem and how Bitcoin system handles this problem. Then, we considered several solutions for BlockChain scalability and analyzed the advantages and disadvantages of the proposed solutions.

All these BlockChain scalability solutions offer a unique way to speed up the transactions and some of them have already been implemented.

Our further research will be focused on examining whether these solutions can truly solve the scalability issue. Also, we will consider other applications of BlockChain, for example in IoT, Machine Learning etc.

REFERENCES

[1] M. Crosby, Nachiappan, P. Pattanayak, S. Verma,V. Kalyanaraman, "BlockChain technology: Beyond bitcoin", Applied Innovation Review, Berkeley, Issue No.2, June 2016.

[2] https://blockgeeks.com/guides/smart-contracts/

[3] Mechkaroska D., Dimitrova V., Popovska-Mitrovikj A: A Survey on Applications of BlockChain Technology, Proc. of the 15th International Conference on Informatics and Information Technologies CIIT, 2018 (in print)

[4] V. Gupta, "A Brief History of BlockChain", https://hbr.org/2017/02/a-brief-history-of-BlockChain, February 28, 2017.

[5] https://www.buybitcoinworldwide.com/confirmations

[6] https://en.bitcoin.it/wiki/Confirmation

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", 2008, http://bitcoin.org/bitcoin.pdf.

[8] https://people.xiph.org/~greg/attack-success.html.

[9] M. Rosenfeld, "Analysis of hashrate-based double-spending", arXiv:1402.2009.

[10] https://en.bitcoin.it/wiki/Irreversible-Transactions

[11] http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

[12] http://learnmeabitcoin.com/faq/segregated-witness

[13] https://cointelegraph.com/tags/segwit

[14] https://blog.bitmex.com/the-segwit-transaction-capacity-increase-update/

[15] https://blockgeeks.com/guides/blockchain-scalability/

[16] https://www.coinbureau.com/review/zilliqa-zil/

[17] The Zilliqa team, "The Zilliqa Techical Whitepaper", https://docs.zilliqa.com/whitepaper.pdf, August 10, 2017.

[18] https://cryptodaily.co.uk/2018/05/zilliqa-zil-answer-blockchain-scalability/

[19] https://cryptocurrencyhub.io/an-introduction-to-consensus-algorithms-proof-of-stake-and-proof-of-work-cd0e1e6baf52