The Evolution of Blockchain – From Chain of Blocks to Direct Acyclic Graphs

Kiran Kumar Kondru,
Ph.D. Research Scholar, Department of Computer Science,
Central University of Tamil Nadu
Thiruvarur, India
kirankondru.tech@gmail.com

R Saranya
Assistant Professor, Department of Computer Science
Central University of Tamil Nadu,,
Thiruvarur, India
saranya@cutn.ac.in

Abstract— ***Blockchains like Bitcoin have introduced a new kind of completely distributed and decentralized currency. These public peer networks allow any user with a computer to transact over the internet without the need of third parties like Banks. But they do have drawbacks with issues like Scalability and Privacy. The adoption of Blockchain Technology and Cryptocurrency necessarily depends on how well a Blockchain scales up/down without breaking or slowing down. As such, here in this paper we discuss how transaction scalability has become the key impediments to the wider adoption of Blockchain technology. For overcoming the Scalability issue, one path of research leads to changing the data organizing structure from a linear chain of blocks to trees to directed acyclic graph. We discuss how incremental innovation in both the underlying data structure and the corresponding consensus mechanisms led to significantly addressing the scalability issue***.

Keywords—Blockchain, Bitcoin, Distributed Ledger Technology , Directed Acyclic Graph, GHOST, SPECTRE

I. INTRODUCTION

Traditional ledgers which keep record of transaction between two parties have been maintained by a trusted third party. This record can hold transactions of money between two individuals or transfer of land deeds from one person to another and so on. The need for a third party record keeper arises due to lack of trust between individuals and the third party provides for it. The third party maintains a record of transactions, in return charges a fee on both parties. Now-a-days, Banks are most commonly trusted 3rd parties which facilitate transaction between individuals in return charging a fee. Though inventions like Computer and the Internet changed a lot even in Banking, the same old completely centralized model of recording transactions. Bitcoin, the first Blockchain, came up with a unique and innovative solution to this centralized ledger by introducing a cryptocurrency on top of a peer network. In this P2P network each node(computer) has a copy of the whole ledger of transactions and every node can verify every individual transaction done by its members

A Peer to Peer (P2P) network is autonomous and self-organizing, with clients free to participate and leave the network. This is unlike a traditional distributed system. All the peers in the network offer a combination of online services and is voluntary in nature. P2P communication involves two equal role users. P2P Computing is a method which takes advantage of computational and content resources usually to complete a huge tasks[1]. In P2P Computing there is no requirement for coordination by a central server and no peer has a total view of the entire system. Peers act as both servers and clients at the same time sharing services and resources directly with each other.

The common characteristics of a typical P2P system are

1) *Decentralization:* No central server is involved, and peers have a partial view of the entire system to construct the overlay network[1]
2) *Self-organizing:* Resources in P2P system are dynamic in nature and fluctuate. There is no need for a central management system to manage these resources.
3) *Ad hoc Connectivity:* Availability of peers is not guaranteed. The overlay topology changes frequently and the system as a whole scales rapidly. P2P systems should be able to provide even in such dynamic situations.
4) *Anonymity:* Anonymity is provided when two peers communicate through one or more intermediate peers.
5) *Scalability:* In a P2P system there is no single point of failure as each peer shares resources directly with each other while each peer keeping a limited number of system states. These features enable high scalability.
6) *Fault Tolerance:* All peer are equal and same resources could be stored in multiple peers. These features facilitate fault-tolerance.[1]

II. BACKGROUND ON BLOCKCHAIN

A. How the Blockchain Works - Bitcoin

Bitcoin[2] was introduced by Satoshi Nakamoto in a white paper. It is a cryptocurrency which is completely decentralized. Bitcoin protocol works on a distributed peer to peer network over the Internet where the nodes can transact over it through the use of its native currency called Bitcoin. Bitcoin achieves true decentralization by having each node in the peer network to have a copy of the transactions ledger. Through this decentralization Bitcoin eliminates single point of failure, since there is no single server or database to corrupt by malicious users.

The ledger is shared across the peer network. The current state of the ledger has to be synchronized with every node in the network. Since every node in the network has a copy of the ledger locally on the node, every node can verify any of the new transactions that are broadcast over the network. Verification is done by going through all the transactions in a chronological order a user did over time from the beginning. By doing this any node could tell whether the user's account has sufficient balance and whether to approve of the new transaction or not.

Bitcoin bunches together transactions into blocks of fixed size and make blocks point to preceding block in the chain. The first block is a special block called Genesis block and it is created only once. Once a block is verified by all the nodes in the network, they add that block to their own local copy of the linked chain of blocks. This is called a Blockchain. Bitcoin makes these blocks such that they are immutable once that block is accepted by the whole network. That is its contents can't be changed. This is achieved through cryptographic hashes. The transaction that form a block are hashed first and these hashes are then formed into a Merkle tree. The advantages of a Merkle tree of hashes is that if a single transaction in the block is changed, it's hash changes and so does Merkle tree root hash, which is easy to verify by the other nodes. The blocks are linked by the hashes like a linked list, the latest block being added at the end of the chain of blocks. If a malicious user tries to change a single transaction, he would have to change all the hashes of the blocks which came after that block and convince the rest of the nodes that his chain of blocks should be replicated by all, which is a very difficult task.

Since the Bitcoin network is a leaderless distributed peer-to-peer network, the nodes must arrive at a consensus for as to acknowledge the state of the distributed ledger. Only when consensus is reached can the ledger be synchronized across the network. This, Bitcoin achieves by making nodes compete to create a block while also verifying the transactions in the block are legit by rewarding them with some Bitcoins. Apart from verifying the transactions (which all the nodes do anyway), the competing nodes have to come up a computationally difficult puzzle of coming up with a hash of the block with some leading zeros. This is known as Proof-of-Work (PoW) Whoever achieves this task first would broadcast over the peer network the hash and the new block created. The rest of the nodes verify the hash with the newly created block and add that block to their copy of the Blockchain. This computational puzzle (PoW) and the incentive or reward system together encourages verification by nodes in the network and dissuades malicious use of the network.

B. The Double Spend Problem

But there is a possibility of malicious users trying to misbehave in the network, especially by trying to create a what is known as a double-spend scenario. A double-spend attack[3] is where a user tries use a spent coin in another transaction. In the Bitcoin network, the blocks are added sequentially. Multiple winners can be there at the same time winning the PoW computation puzzle. As there are multiple winners there being multiple blocks pointing to the same parent block. And oncoming blocks subsequently attach to one of the many blocks and they form their own chain. These are called as side chains. Fig 1 illustrates this concept. But Blockchain is a sequential data structure and not a tree. To resolve this, Nokomoto Consensus[2] states that the longest chain will be the permanent chain to be replicated across the Bitcoin Network. The side chains so formed will be discarded overtime by all the nodes in the network and stick to the longest chain rule. For all practical reasons after 6 blocks are added to the chain it can considered as the permanent chain.

An attacker has to win the PoW puzzle and create a block without his transaction in it. And he has to keep on winning PoW for the next consecutive 6 blocks such that his chain becomes the longest chain and gets permanently recorded. Since his transaction is not recorded, he can spend the same money in another transaction. But since winning PoW is probabilistic anyone can win and add blocks to the main chain. As such for a malicious user to double spend he has to have at least 50 percent of the total computing capacity of the network, which is practically not feasible as there can be thousands of nodes in the network. PoW is computationally difficult and the difficulty of the puzzle automatically adapts such that only one block is created for approximately 10 minutes. This time span allows a block to reach even geographically distant nodes in the worldwide peer network.

C. Limitations of the existing Blockchains

Some of the major limitations of Blockchains based on Proof-of-Work like Bitcoin and Ethereum[4] are its Scalability and Privacy. In this article we focus on Scalability. As an entire world-wide peer network has to verify and agree on a block broadcasted it will take time for the block to propagate. The Bitcoin protocol is intentionally made such that the Proof-of-Work puzzle is adaptive and adjusts so that blocks are produced only once for 10 minutes in the entire network. Either producing more blocks or increasing the size of the block results in reduced security of the whole network and increased chances of double-spend attacks by malicious users in the network. The inability to increase the transactions per second is the same across many Blockchains (and not just Bitcoin) which use Proof-of-work based consensus including Ethereum. Other consensus mechanisms were designed but they have similar scalability problem. Private or Consortium Blockchains have no need of PoW kind of Consensus and are designed to be less decentralized. This is due to the fact that the identities of the nodes are known beforehand in a private Blockchain and the propagation of incremental change in the state of the Blockchain can be easily achieved using traditional distributed algorithms.

III. EVOLUTION OF BLOCKCHAIN DATA ORGANIZING STRUCTURE

Many different Blockchain consensus mechanisms are proposed and implemented for overcoming this shortcoming of low transactions processing on Bitcoin like

networks. Another route chosen by some researchers is through changing the data organizing structure of the Blockchain itself from a linked-list kind of structure to a tree structure and there to a Graph structure especially the Directed Acyclic Graph. In the following subsections, we discuss how the incremental change in the design of the underlying data organizing structure contributed to increased throughput of transactions while also maintaining the same level of security. The change in the data structure also requires new algorithms for achieving consensus.

As a way of increasing the transaction speeds of the network, bigger blocks can be added, or frequency of block creation can be increased. But either of those solutions (leave alone both of them together) would create more conflicts among blocks, which in turn reduces the level of security from attacks such as double-spend.[5]

A. Tree of Blocks - GHOST Rule

As a way of increasing the transactions an alternative has been suggested to the longest chain rule called GHOST[6] (Greedy Heaviest-Observed Sub-Tree). A variant of GHOST is already been adopted in the Ethereum project. It has been observed that in the Bitcoin's Data structure, a number of side chains simultaneously exist attaching themselves to the main chain. These side chains too are the result of winning the PoW puzzle by the block creators. They form a tree structure as shown in the below Figure 1.

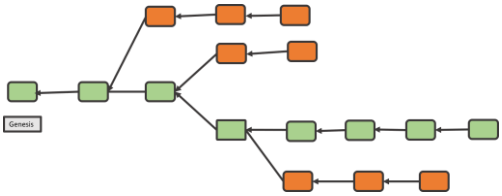

Fig 1: Blockchain with Side chains[7]

The Blocks represented in orange are side chains which are formed when there is more than one winner of the PoW Hash puzzle. Instead of these side chains being removed as per the longest chain rule, the GHOST protocol selects the heaviest sub-tree whenever there is a fork in the chain. Heaviest sub-tree is derived by calculating how many nodes each sub-tree has under it. So, instead of the longest chain, it's the heaviest sub-tree. The sub-tree selection is explained with a diagram below in Fig 2.

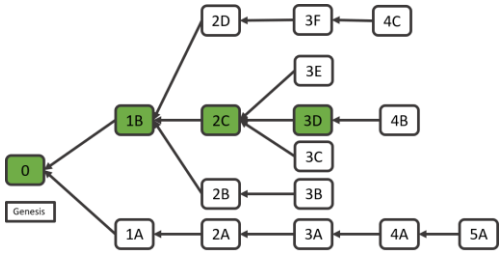

Fig 2: Sub-tree selection[8]

In the above figure Block 1B forms a sub-tree with Blocks 2D, 2C and 2B as its child sub-trees. The side chain 2D - 3F - 4C - 5B form's the main chain according to the longest chain rule, but it's not selected here. It also becomes part of main chain according to the GHOST protocol. Each node will be given a weight of say 1, then the sub-tree 2D has a weight of 4, 2C has a weight of 5 and 2B has a weight of 2. The sub-tree 1B which is a parent of all these sub-trees has a cumulative weight of 11.

An attacker can create a longer chain. Here in the diagram the nodes 1A through 6A form the longest chain which the attacker secretly created. Which might have been a permanent chain. Even then the attacker's chain is not selected and will eventually be discarded. As the nodes try to get selected to be part of the longest chain in the Bitcoin network, so is the heaviest sub-tree like the longest main chain. They try to attach themselves to the sub-tree which is as much centre as possible. Instead of one block being added to a linear chain of blocks, many blocks (which won the PoW puzzle) can be added to an edge block forming a sub-tree. This greatly increases the block creation rate and in turn increases the number of transactions to be processed making the whole network scalable. However, implementations can adjust the rate of block creation as GHOST is designed to be configurable.

Bitcoin network as a reward mechanism for those nodes winning the PoW puzzle. And the transaction fees are also added. In this case only one winner is rewarded. But in the case of GHOST there are multiple winners and the reward is shared. How this reward is shared is left to the implementation. Since the reward is shared, it might not be as profitable.

a) Shortcomings of GHOST Rule:

The problem of computation intensive PoW hashing is not solved. Miners that are better connected to this blockchain network are get a little better rewards than the share of hashing or computation power they have. The selfish mining strategy can be employed here by miners with low hashing power.

B. Block DAG – SPECTRE Protocol

To overcome the security-scalability trade-off imposed by the Nakamoto Consensus, SPECTRE is proposed. Rather than follow a tree like structure, SPECTRE [5] uses a Direct Acyclic Graph (DAG)[9] of blocks. SPECTRE further relaxes node synchronization. And allows the blow to literally grow on the DAG structure almost concurrently. Whereas GHOST more or less follows the main chain concept of the Nakamoto Consensus, SPECTRE altogether loses this. Instead of a main chain, GHOST follows heaviest sub-tree. Instead, SPECTRE has a voting mechanism which determines the order of any pairwise blocks. Though blocks may be incorporated in the DAG; the individual transactions might still get rejected. As such, it can be said that

SPECTRE allows for robustness of blocks but not for robustness of transactions.

The key contributions of the SPECTRE protocol according to the[10] are (1) SPECTRE is inherently scalable and (2) a formal framework for cryptocurrency payments is developed. The main technique used in the protocol is of the voting algorithm. It specifies the order of each pair of blocks in the algorithm. According to it, each block votes on the relative order of not only their parent blocks but also their descendant blocks Here voters are blocks and not nodes(miners). The vote of each block is interpreted algorithmically according to its location within the DAG. Majority's aggregate vote becomes very fast and use this majority vote to extract consistent set of transactions.

SPECTRE does better with Block Withholding attacks that a Bitcoin network is prone to. It's also known as Selfish mining[11]. In this kind of attack, a miner would generate a block but would not broadcast it. The simplest form of this attack is called Finney Attack. The attack is a variation of double spend attack. An attacker would generate a valid block but would not broadcast it and then he would broadcast a transaction as a payment for a service. The merchant will see the transaction and sees nothing connecting in it and will confirm the transaction. Just right after that the attacker will broadcast the generated
blocks with a second transaction which will conflict with the first transaction. The Bitcoin network will accept the block and invalidate the first transaction, as if the first transaction never occurred.

With SPECTRE's vote based pairwise ordering attackers creating secret chains cannot win votes by the existing blocks from honest nodes. The pair-wise voting mechanism is illustrated below in Fig 3.

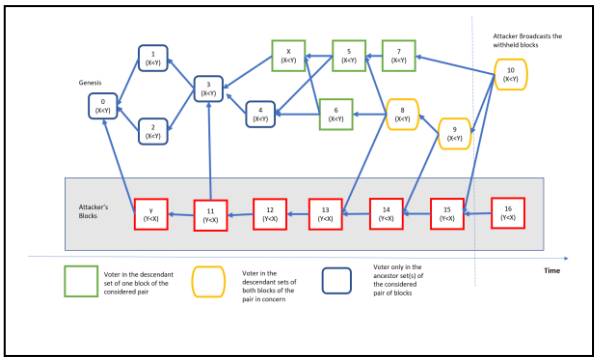

Fig 3: SPECTRE's vote-based pairwise ordering[6]

In the above figure Fig 3, we consider X and Y blocks and the relative ordering is voted by other blocks. Blocks which are descendant blocks of X will vote as X precedes Y as they see more blocks with the same vote X precedes Y in their ancestor blocks and they see only X. Blocks 0 - 4 will vote X precedes Y since they see more of the same vote in the descendant blocks. Blocks 8 - 10 which have both X and Y as ancestors run a recursive query to their predecessor sets and use the majority voting results as their own votes. In the above figure, the attacker though has the longest chain which says that Y precedes X, they cannot win the votes from existing honest blocks because of the lack of connection to the existing blocks.

Here the block creation rate is accelerated as more blocks can be added to the network as there are more honest miners creating those blocks. This is also one of the basic observations of the protocol that there are a greater number of honest miners than malicious miners. As the number of nodes grows in the network the block creation also increases.

As SPECTRE is able to increase transaction throughput as the network grows, it makes it more scalable compared to other liner chain based blockchains. Casanova [7] is one of the blockchain platforms that use this concept of blocks in a DAG as their data organising structure.

a) Shortcoming of SPECTRE

SPECTRE protocol can be very fast without
any conflicts in the network. But with visible double-spend transactions the same speed is not guaranteed. Since SPECTRE uses pairwise ordering it's only suited to support cryptocurrencies where strict ordering of transactions is not necessary. If 2 transactions are done by a user, and they are not ordered accordingly, those two are still valid transactions as long as the balance in the account is not zero. But that is not the case when Smart Contracts are used as in Ethereum [3]. e.g., A smart contract contains code for booking an airline ticket. Airlines issue tickets on first come first served basis. And if the smart contract of two different users are not in order, the first and second user's request might get interchanged and a genuine first user might not get a flight ticket, though he is first to issue the smart contract. In such cases, SPECTRE might not be
appropriate.

C. Transaction DAG – IOTA's Tangle

IOTA[12] Platform takes a different direction to solve the problem of scalability using DAG by totally doing away with the concept of blocks. the DAG in IOTA is called as Tangle[ref]. And each transaction is a vertex in Tangle and each edge (directed) is an approval of that transaction. Every new transaction (vertex) has to approve (edge) at least two new transactions in the Tangle. The same transaction itself will get validated by incoming transactions (vertices).

The idea of sequence of blocks along with Proof-of-work is abandoned. But PoW with simpler hash is used to prevent spamming the IOTA network with transactions. IOTA is mainly designed for Internet of Things and aims to make machine to machine communication and transaction easier. IOTA also has its own cryptocurrency called iota. Unlike Bitcoin network which rewards miners with Bitcoin for successfully solving the PoW puzzle, all iotas are created once in the Genesis block and no more iotas will ever be created.

In the Bitcoin network, miners grouped together and try to win every hashing puzzle and share the reward among themselves. These groups thus have become more powerful and have control over what transactions to choose. Transactions offering higher transaction fees might get chosen among all the transactions generated in the time period.

In the IOTA's Tangle structure every incoming transaction (vertex) has to validate two existing transactions, thereby eliminating miners altogether. Here every node participates in validating and hence contributes to the security of the whole network. Also, because of the lack of miners and the whole mining process, the transactions could be smaller with absolutely no transaction fee. The IOTA network is deliberately designed that way.

Once a transaction is approved (edges) by a large number of transactions (vertices) either directly or indirectly, that transaction becomes part of the Tangle DAG permanently and is practically impossible to change. Newer transactions coming into the DAG have to still get approved two other incoming transactions. However, transactions belonging to the same user can validate their own transactions and can lead to Double Spending. To avoid this IOTA has a tip selection algorithm. IOTA performs a random walk from Genesis to tips (Edges) and stops only when it reaches leaf's node. This walk is done twice, and 2 tips are chosen by the algorithm for the incoming transaction to validate.

In the IOTA Network, the random walk is done by Random Walk Monte Carlo (RWMC) algorithm. The goal of this algorithm is to generate fair samples from the distribution. This algorithm is used for choosing two tips (vertex) while creating a new transaction and to determine if a transaction is confirmed.

This walk is biased towards transactions with more cumulative weights. The cumulative weight of a transaction is the weight of transaction itself plus the sum of weights of the all the transactions that directly or indirectly approve this transaction.

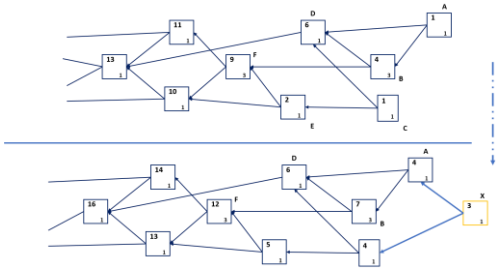

Fig 4: IOTA’s Tangle[12]

In the figure the South East number is the cumulative weight. Transactions A, B, C and D have cumulative weights of 1,4,1 and 6 and a new transaction X with a weight of 3 comes in and approves A and C. Now the cumulative weights of A, B, C and D has increased to 4,7,4,9. Once a cumulative weight reaches a thresh-hold value, the transaction is said to be confirmed.

Here in the IOTA Network, a Proof-of-Work is employed too. But the hash puzzle is not as hard as the Bitcoin's since IOTA is mainly designed for the IoT devices which have limitations on computing and storage. This PoW is mainly used for preventing Spam and also to prevent Sybil attack[13].

The Tangle DAG can be said to be a transaction DAG and is a new design with associated algorithms for consensus. As the network grows and the number of transaction increases, the IOTA network not only accommodates it but also makes the network faster and more secure. Each node with a new transaction will be participating and validating transactions. This marks a great shift from the original Blockchain with a chain of blocks.

1) Shortcomings of IOTA’s Tangle: Due to the smaller initial size of the IOTA network taking over the whole network by taking over more than 33 percent of the nodes. This is comparatively easier than the 50 percent computational power required to overtake a PoW network like Bitcoin. IOTA introduced to a stop gap measure by introducing some centralization with nodes called Coordinators which are spread all over the network. Though the PoW used in IOTA is computationally less intensive, it still consumes some computational resources and in IoT devices it might prove costly. IoT devices generally are resource constrained. Other famous Blockchain platforms like Obyte[14] (previously Byteball) and Nano[15] (formerly Rai Blocks) use a little different design trying to overcome the shortcomings of IOTA network. Obyte uses witnesses to verify transactions Witnesses are individuals deemed to be trustworthy and their identities publicly known. Once a transaction is added to the ledger, it must be seen by a majority of the witnesses. This is in contrast to IOTA's Coordinators.

IV. CONCLUSION

In this paper we have discussed how the search for more scalable blockchain technology has led to incremental innovations on the existing Data organizing structure and the associated consensus mechanisms. GHOST is a small increment. It made a change to the longest chain rule and created a tree of blocks. SPECTRE introduced DAG of Blocks with pair-wise voting mechanism. While IOTA completely abandoned the idea of Blocks altogether and achieved DAG of transactions. This greatly increased transaction throughput while also being secure enough to be used as a public Distributed Ledger Platform.

Scalability is utmost important in a public blockchain which involves hundreds or thousands of nodes or more on a public worldwide network, where the identities are not known beforehand, and the nodes can join and leave as they wish. We believe that only with increased transaction throughput can a public blockchain, which is

completely decentralized, be successful and be more accepted by the people and companies.

REFERENCES

[1] J. J. D. Kai Hwang, Geoffery C. Fox, *Distributed and Cloud Computing - From Parallel Processing to the Internet of Things*, vol. 112, no. 483. Elsevier, 2012.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *White Pap.*, pp. 1–9, 2008.

[3] U. W. Chohan, "The Double Spending Problem and Cryptocurrencies," *SSRN Electron. J.*, 2018.

[4] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger. EIP-150 REVISION," *2017*, no. August 1, 2017, p. 33, 2017.

[5] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8975, pp. 528–547, 2015.

[6] A. Z. Yonatan Sompolinsky, "Secure High-Rate Transaction Processing in Bitcoin," in *International Conference on Financial Cryptography and Data Security*, 2015, vol. 125, no. 6, pp. 507–527.

[7] G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 101–128, 2018.

[8] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, no. Vm, pp. 22328–22370, 2019.

[9] Wikipedia, "Directed Acyclic Graph."

[10] Aviv Zohar, Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Serialization of Proof-of-work Events: Confirming Transactions via Recursive Elections," *Medium*, p. 66, 2017.

[11] I. Eyal and E. G. Sirer, "Majority Is Not Enough: Bitcoin mining is vulnerable," *Commun. ACM*, 2018.

[12] S. Popov, "IOTA whitepaper v1.4.3," *New Yorker*, vol. 81, no. 8, pp. 1–28, 2018.

[13] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack," p. 259, 2004.

[14] A. Churyumov, "Byteball : A Decentralized System for Storage and Transfer of Value," pp. 1–49, 2017.

[15] C. Lemahieu, "RaiBlocks : A Feeless Distributed Cryptocurrency Network," pp. 1–8, 2016.