 doi:10.20944/preprints201910.0071.v1

Article

Challenges and Emerging Solutions for Public Blockchains

Victor Holotescu * and Radu Vasiu

University Politehnica of Timisoara, Romania; radu.vasiu@cm.upt.ro
* Correspondence: victor.holotescu@yahoo.ro

Abstract: With the interest and attention that the Blockchain and the Distributed Ledger Technologies (DLTs) have recently demanded, the technology is advancing at a very high rate. With investors and applications in a wide variety of fields, a lot of funding and efforts are being driven into bringing the technology to everyday use. The community and companies are coming up with new ways to collaborate, which makes the blockchain ecosystem evolve at full tilt. Consequently, this paper's aim is to review the academic and grey literature and to provide readers with information about the evolution, benefits and challenges of the Public Distributed Ledger Technologies and to discuss the latest solutions, which are being developed for bringing decentralization closer to the mainstream. The paper reviews the Directed Acyclic Graph (DAG) structured distributed ledgers with focus on the Hedera Hashgraph, a novelty DLT bringing a unique consensus algorithm with new use-cases enabled by new cryptoeconomic mechanisms, as well as vital services, such as Solidity smart contracts and distributed file storage. Then, we are going to explore second-layer network protocols, a major topic for solving scalability issues and for decentralizing cryptocurrency exchanges. The article tries also to identify the particularities of these technologies and how they bring specific answers to the blockchain trilemma, consisting in three themes - scalability, interoperability and sustainability.

Keywords: Blockchain; distributed ledger technology; blockchain trilemma; scalability; interoperability; sustainability

1. Introduction

Since Satoshi Nakamoto published the paper about Bitcoin [1], a trustless peer-to-peer network, in 2008, and since he has turned on the blockchain by mining the genesis block one year later, the technology has proven to stand out, making it possible to disrupt the future of many fields. The blockchain benefits brought by its distributed, transparent and immutable nature make possible use cases from Finance, Banking, Business and Supply Chain to Education, Media and Health [2–3].

During this period, blockchain projects have been very well funded, with $22.5B in Initial Coin Offerings (ICOs) by the end of 2018 [4], which have been proven to have a high risk of participation, with many international initiatives meant to accelerate the adoption and awareness of Distributed Ledger Technology and Digital Currency [5–8], and with trusted launchpads for funding new promising blockchain solutions through Initial Exchange Offerings (IEOs). With all the attention that blockchain technology has received, it still hasn't overcome its biggest hurdles in order to be ready for mass adoption, making its shortcoming widely debated, resulting in new solutions to be developed and explored.

In this paper, we are going to introduce the blockchain technology, talking about its history and know-abouts. The first subject to be discussed is related to the limitations of public blockchain technologies and why trying to improve on any of the characteristics of scalability, interoperability and sustainability, referred to as the blockchain trilemma, will affect the true value and the benefits of the blockchain [9]. The next topic examined will be the Directed Acyclic Graphs (DAGs), an alternative structure for blockchain, where we are aiming to introduce and provide insights on the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

different solutions using this kind of DLT, concentrating on Hedera Hashgraph, a unique patented network, which has to offer the whole set of decentralized services and new cryptoeconomic mechanisms, that bring a new level of fairness, speed and security to the decentralized space. Ultimately, the paper will review the second-layer networks aiming to scale blockchains, exploring upon others the Lightning Network. This is an off-chain protocol, starting as a Bitcoin Improvement Proposal (BIP) [10], which is implemented by using Hash Timelock Contracts (HTLC) and which can be extended on blockchains with time-locks and multi-sig capabilities, providing interoperability solutions as well. Throughout the paper we are going to see the types of Decentralized Applications (DApps) that are being developed on Hedera Hashgraph and the Lightning Applications (LApps) built on the Lightning Network. By the end, we are going to identify the next steps for moving forward with the technology, finishing up with the conclusions raised throughout the paper.

The paper is a literature review realized by analyzing academic journals, conference papers and grey literature (online articles, videos, newsletters, forums, e-mail archives, etc.) with the aim of encompassing the decentralized ecosystem, from the formal academic perspective and also from the more approachable means where the blockchain has its roots.

2. Concepts

2.1. Definition

There are many ways in which the Distributed Ledger Technologies (DLTs) and the Blockchain have been defined, so as to suit different levels of knowledge and understanding and also to better encapsulate the essence of technology and its capabilities.

A concept existing from 1982, Distributed Ledger Technology (DLT) designates multi-party systems being able to withstand environmental adversaries, meaning that the network of independent participants can continue to work correctly with no central operator or authority, despite unreliable or malicious parties [11].

The Blockchain is a type of DLT, an append-only chain-like data structure, made out of signed and timestamped blocks that contain the transactions. Nodes called miners are participating in a consensus mechanism, and are responsible for validating transactions, with which new blocks are created. A transaction may involve the transfer of tangible or digital assets, or the completion of a task. Blocks are identified through a cryptographic hash, each of them containing its own hash and the hash of the previous block, creating the chronologically ordered blockchain structure [12].

The Distributed Ledger Technologies create a robust, auditable, secured and efficient environment, while establishing the self-sovereignty and eliminating the third party control [13].

2.2. History

The blockchain technology came to life by bringing together technologies that have been proposed and published in different papers over the last 40 years. During the 1980s, David Chaum defined blind signatures [14] and the first electronic cash protocol [3], which solved the anonymity and double spending problem in a centralized matter. In 1997, Adam Back introduced Hashcash [1], where, as a security measure for sending spam mail, the attackers had to solve a computational puzzle that was easy to verify, but hard to generate. This is the main concept of the Proof-of-Work protocol, which was first proposed by Wei Dai, when he discussed B-money [15]. The mechanism he described was lacking node interaction in the consensus and security. Nick Szabo [16], with his proposals on Bit gold, improved the mechanisms' security by adding the difficulty of the computational puzzle to be solved.

In 1999, Tomas Sander and Amnon Ta-Shma [17] brought the Merkle tree structures and Zero-Knowledge Proofs, while in 2004 Hal Finney [18] defined what he called the Reusable-Proof-of-Work (RPOW) consensus mechanism by incorporating Hashcash. What the whole infrastructure was missing from what we know today as blockchain is the peer-to-peer network, the last piece of the puzzle, which was added by a person with the alias Satoshi Nakamoto, in the form of Bitcoin, the peer-to-peer electronic-cash system [1].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

2.3. Blockchain Types

The Blockchain has evolved into different categories, each of them having its benefits and downsides.

Private or consortium blockchains are those in which the nodes maintaining the ledger are permissioned to participate in the consensus, either by being centralized inside the entity running the blockchain or by going through Know Your Customer (KYC) and Anti-Money Laundering (AML) processes. Thus these blockchains are semi or fully centralized and are useful for auditability. Private and consortium blockchains have restricted access, with fewer and known upfront nodes participating in the consensus, these protocols for closed sets being faster than those for open networks. At the same time, being in a closed environment, some private blockchains will have issues interoperating with other networks, so the benefits are minimal [19].

Another type of blockchain are the public permissionless blockchains, which are run by thousands of nodes, anyone being able to set up a node and start participating in the consensus process. While it is likely for bad actors to join in, it is practically impossible for them to take over these blockchains, as that would require a huge financial investment. That is why public blockchains are considered to be tamper-proof [2]. Bitcoin or Ethereum are the best-known blockchains in these category, examples of public blockchains being mainly discussed in the paper.

Hybrid (or federated) blockchains started to be developed as they can integrate the security of the public blockchains with the privacy and speeds of the private or consortium blockchains [12].

2.4. Consensus Mechanisms

The blockchain is run by a consensus protocol meant to solve the Byzantine Generals Problem [20], where nodes need to make the right decision, given that there might be malicious actors participating in the process. Nodes are incentivized to run these consensus mechanisms, being rewarded whenever they validate the transactions and add a new block, while also being heavily penalized whenever they try to add an invalid transaction to the blockchain. With all the mechanisms set into place, the consensus protocol is the main point of failure of a blockchain, as its failure compromises the ledger.

There are multiple types of protocols which have been developed to run in different scenarios for public and private blockchains and also for other types of DLTs. The ones used successfully by the major public blockchains are Proof-of-Work, Proof-of-Stake and Delegated-Proof-of-Stake [12].

Proof-of-Work (PoW) is the consensus mechanism which runs on Bitcoin and Ethereum, with different implementations called Hashcash and Ethash respectively. This protocol has proven to be the best solution for solving the Byzantine Generals Problem, making it the most secure consensus mechanism.

The nodes, called miners, participating in the consensus have to solve a computational problem of a certain difficulty. Whichever miner solves the computational problem first will add the next block to the blockchain. The computational problem refers to the generation of the hash identifier of a block, where the difficulty dictates the condition under which the hash is valid. Regularly, this means the hash has to be lower than a certain number and, thus, preceded by a certain number of zeros. When the block is added to the blockchain and broadcasted to the network, the node that solved the problem is creating a new transaction, which transfers the mining reward to its address [21].

In order to gain control over a blockchain maintained with a PoW consensus mechanism, a malicious attacker has to take over more than half of the nodes participating, in a 51% attack, thus making the PoW the most secure consensus protocol ever developed.

Proof-of-Stake (PoS) has been developed as a solution for the high volume of energy consumed in the process of PoW and it is based on nodes proving ownership over their tokens to generate blocks. The most common practice for PoS is for the system to choose a random leader, based on its stake in the network, which creates the block. The mechanism works because having more currency makes it less likely for a node to be malicious. All malicious nodes trying to alter the state of the blockchain are penalized by having their tokens taken.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

Delegated-Proof-of-Stake is the protocol used by EOS, Steem, Bitshares, Ark or Lisk, the first two blockchains having lately become very popular for building decentralized applications. Blocks are created by block producers and validated by block validators. Block producers are elected every round by the nodes inside the network, based on their stakes. While block producers can also fine-tune their block creation intervals and the block size, having a smaller pool of block producers allows a higher transaction throughput, while it is considered to be more centralized compared to the other consensus mechanisms [22].

Nowadays people are using Distributed Ledger Technology and Blockchain interchangeably even if DLTs represent different technologies, one of which is the Blockchain.

Although the two technologies are solving the same problem and trying to bring the same amount of benefits, of providing decentralization by potentially reducing the most important regulatory role of being a middleman in our society [13], the term of DLT has started to gain more popularity because of the new technologies developed for overcoming the limitations of Blockchain. We will present these technologies in the section on the Directed Acyclic Graph (DAG), where we are going to discuss the unique Hashgraph slgorithm developed at Swirlds.

3. Challenges

With blockchain becoming so popular, and with everybody trying to build the decentralized applications which will turn the technology mainstream, there are still many challenges for public blockchains, aside from the fact that the blockchain should be integrated in the current legacy centralized system. The challenges of the public blockchains are related to Scalability, Interoperability and Sustainability, coined in 2018 as the blockchain trilemma by Vitalik Buterin, the creator of Ethereum, referring to the difficulty of creating a blockchain with the three characteristics at the same time [23]. Currently, there is no fully working blockchain to have solved all these issues and it is considered that you can only address two of them by giving up the other one [24]. That is why multiple blockchain platforms exist: to offer the best possible solutions for specific use-cases. In what follows, we are going to talk about these three challenges, while later on we are going to see possible solutions to them.

3.1. Scalability

A public blockchain should respond to the critical challenge of scalability, which means to achieve the consensus of the distributed computing nodes in a scalable and efficient manner.

In the blockchain, all the nodes are involved in creating blocks that can be added to the ledger and they decide whatever unconfirmed transactions they want to include in the block they are working on. The node which calculates the first valid hash in PoW or the declared leader in PoS or other consensus mechanisms is going to forge the new block and then the block needs to be broadcasted to the whole network. A new block of 1MB for Bitcoin is propagated every 10 minutes, giving it a throughput of 7 transactions per second (tps), while Ethereum can confirm 20 tps [24].

Small adjustments have been brought to the blockchain in order to address scalability issues, such as increasing the block size of Bitcoin, which is 1MB, to 4 or 8MB. A hard fork in the main Bitcoin blockchain has been created, called Bitcoin Cash, having an 8MB block [25]. While this adjustment can increase the number of transactions that can be stored on a block, the block will take longer to propagate in the network, as nodes require better internet connection with larger bandwidth.

In the case of maintaining the size of the blocks, transactions with higher fees are validated faster, as miners have the ability to choose the transactions they want to mine, in order to gain higher rewards. This will unfairly cause the neglect of low fee value transactions, as the blockchain might not follow a first come first served rule. A solution for scalability is the SegWit (Segregated Witnesses), another fork in the Bitcoin, which eliminates different signatures from the blocks, thus allowing the addition of more transactions [25].

To gain a better performance in scaling the blockchain, research has been conducted to address the problem by creating new data structures, such as Directed Acyclic Graphs (DAGs), or more

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

efficient consensus algorithms, or to move transactions and computations from the blockchain to a second-layer protocol.

While looking for solutions for replacing the computation puzzles in PoW with more useful ones, many blockchains are trying to replace PoW with PoS, or to integrate PoS with PoW. The Ethereum team has been talking about replacing PoW with PoS since 2014, and wanted to replace Ethash with Casper protocol, which we currently see integrated in Ethereum 2.0 (Serenity), an early version of Ethereum, built from scratch, using the PoS. For this new version of Ethereum, Vitalik Buterin states that it will validate transactions with 1% of the energy consumed by PoW [26].

3.2. Interoperability

With the persisting problems of scalability and the variety of approaches to solve them, the market has got up to more than 2700 cryptocurrencies in September 2019 [27]. The problem raised is that, with so many different implementations, and with many of them having their own adopters, blockchains will have to be able to share information with each other. This means that transactions could span multiple blockchains and information on a blockchain could be retrieved and validated through a transaction on another blockchain [28]. In [29], Hardjono et al. talks about what blockchains should look like in order to achieve interoperability, referring to the main goals of the Internet architecture and how they should be applied on the blockchain. One of the examples built with the Internet architecture goals premise is MIT Tradecoin. Another project proposes the Digital Trade Coin [30], a cryptocurrency to replace cash money with a worldwide stable digital token, serving as a "blueprint" for an interoperability model between blockchains.

3.3. Sustainability

Sustainability refers to the ability of public blockchains to remain a viable solution over time. A blockchain has to be environmentally friendly, efficient, while its entities should be able to govern over the blockchain in a decentralized manner, in order to take actions in case unlawful acts are being committed [24].

As blockchains are mostly open-source and maintained by communities of programmers and advisors, in order to be successful and sustainable, Decentralized Autonomous Organizations (DAOs) or Decentralized Organizations (DOs) can integrate the ways in which a blockchain should be maintained and governed, keeping the blockchain up-to-date, secured and running for the good of the system.

Many of the current blockchain projects are implemented by companies and corporations that make the decentralized public blockchain mostly centralized, due to the fact that these companies are deciding the roadmaps of the implementations.

Blockchain protocols are actively improved and nodes have always been incentivized to participate in the consensus, but the community and developers have been trying to find ways to improve the system in their own time. New business rules need to be applied to decentralize companies and corporations and also to govern a blockchain like Bitcoin, to reward the individuals proposing enhancements and developing them towards improving the system. A DAO can dictate the economy that incentivizes community participation, which can speed up the implementation of new technology.

Even if many blockchains are better than Bitcoin in some ways, besides not being the first coin to have ever come out, they are not community-driven and thus, despite the decentralized technology they have to offer, they still remain somehow centralized.

Nodes have to keep the ledger with the full history of the transactions. In Ethereum, nodes are holding smart contracts data, and smart contracts transactions need to be run by every node in the network. In September 2019, the size of the Bitcoin ledger was 240GB [31], while the Ethereum full-history ledger was 3.1TB [32].

On top of this, Bitcoin has proven since its appearance that PoW works best in achieving consensus, even if it wastes a lot of energy. With that being said, at the moment of writing this paper,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

there are four mining companies which make a majority in the consensus of Bitcoin [33], and the only way is to become more centralized.

Another downside of the PoW protocol is that a lot of energy is wasted. Bitcoin has an estimated annual consumption of 54.6TWh [34], it consumes more energy than countries such as Romania or Bangladesh. At the same time, the profit of miners is well beyond $1B.

This shows that current consensus mechanism implementations are causing big sustainability issues. Eventually, if we envisage a long-lasting life for blockchains, and a better behavior than Visa which has 24000tps [35], keeping a copy of the whole blockchain on each node might not be the best solution, as Bitcoin's ledger is gaining 50GB per year. If this technology will be used by people, this number will only increase. Solutions have been proposed, such as MimbleWimble by Tom Elvis Jedusor [36], which can be built on top of Bitcoin and, besides the extra privacy of the account balances, it doesn't maintain the whole blockchain history; therefore, the implementation would reduce the size of the ledger from 80GB, the size of Bitcoin in 2016, to 30GB. There are currently 2 separate implementations that build a new blockchain based on MimbleWimble: Grin, community driven, and Beam, which is financed and run by a company [37]. Other implementations involve lightweight clients, where old transactions are removed from the ledger and nodes hold reference only to non-empty addresses [38]. In the next section we are going to talk about how DAGs and Hedera Hashgraph have addressed this problem, and why DAGs might be superior and the best choice for moving forward.

4. Solutions to Overcome Blockchain Trilemma

4.1. Directed Acyclic Graphs

Directed Acyclic Graphs, also known as DAGs, are a type of DLT meant to solve the trilemma issues of the blockchain. A DAG is a structure composed of vertices and edges that grows in only one direction, edges not referencing previous ones, thus being acyclic [39]. A type of DAG in a technical scenario is a git repository, where new branches or merges can be made, this way creating an acyclic graph.

DAGs can accommodate new consensus mechanisms, other than the ones we can find in the blockchain, which can equally lead to solving the energy consumption problem of PoW.

There are already some implementations of DAGs in an experimental state, as they didn't have the time to prove their security. The most known implementation is the Tangle [40], developed by IOTA, which is designed to overcome the scalability of blockchains and acts as a great candidate for IoT applications. Each node making a transaction or a so-called site, needs to validate two other transactions, called tips, which haven't been confirmed yet. IOTA is a lightweight solution, as nodes do not need to have a full copy of the ledger. On top of this, the more transactions made on the IOTA protocol, the faster the confirmations are. Bramas [41] proposes a model to analyze the scalability and security of the Tangle, suggesting that double spending transactions can be done on the DAG, with more hashing power by the byzantine node. Moreover, the model talks about the coordinator node which is part of the current IOTA implementations. Without the coordinator node, since nodes can validate transactions only by knowing a part of the ledger, called a sub-DAG, a byzantine node can create a sub-DAG that is afterwards accepted in the main DAG and validated by others.

Another implementation is Byteball [42], a DAG which emphasizes 12 witnesses, represented by trusted companies selected by users. Witnesses have to consistently make transactions on the so-called Main Chain, where they post units sequentially. The token is called byte, and a byte is equal to 1 byte of permanent storage on the DAG.

Holochain [43] is another solution to replace blockchains, where different nodes, called agents, hold the state of their own transactions in a personal ledger and at the same time broadcast them through a Distributed Hash Table (DHT) to its neighbors. It is made of multiple shards of DHT, so whenever your agent is offline, other agents may retrieve the transactions you have made through the DHT, similar to BitTorrent. Agents run the so-called DNA, a file containing the validations rules; whenever a new transaction shows up in the DHT, the agents can validate the transaction through

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

their DNA; if the results do not match, the transaction will be shared with the network as being malicious. Holochain is a framework for building decentralized applications and also blockchains, by changing the DNA. Like the other solutions, Holochain is lightweight and can also run on mobile devices.

It is a common assumption that DAGs rely on the fact that, with time, the value of the DLT will increase, in which point the network will become tamper-proof, meaning that a node needs an unrealistic amount of value and hashing power to tamper the structure. At this point, the mechanisms put into place by this implementation at the early stage can be removed, making the system work independently without being centralized. IOTA proposes to eliminate the coordinator node in the future and Hedera Hashgraph, the DLT addressed in the following section, also has some limitations which will be removed with time.

4.2. Hedera Hashgraph

Hedera Hashgraph is designed by Leemon Baird and is an efficient consensus mechanism that makes transactions reach finality very fast, while keeping the time and order of transactions fair, with no security tradeoffs [44]. The patented algorithm is the first Asynchronous Byzantine Fault Tolerant consensus mechanism, designed and delivered by Swirlds, Inc. and it has been mathematically proven through Coq, a proof management system developed at INRIA [45].

The system is a DAG running a Proof-of-Stake consensus mechanism, where nodes are gossiping events to each other, during rounds, at the end of which virtual voting is done to validate the transactions. The network runs a so-called gossip-about-gossip with virtual voting algorithm, that allows every member of the network to be part of the consensus through proxy staking.

Hedera provides services such as cryptocurrency, smart contracts written in Solidity and a file storage, where files of any size can be appended to the ledger.

By gossiping events to each other, every node will find out what the other node know. Nodes hold an image of the same hashgraph history, containing all the confirmed events and transactions, while also knowing which events have been gossiped, to whom and when. By gossiping events to another node, the same transaction will be doubled and contained in another event of another node. When the virtual voting round is over and transactions are confirmed, the time of the transactions, the consensus timestamp, will be defined not by the average timestamp, but by the timestamp situated in the middle of the whole timestamp list for a specific transaction. In this way, Hedera Hashgraph assures a fair timestamp ordering of the transactions.

Timestamps are given by the clock on each computer running the nodes, which assures that if more than two thirds of the network have reliable clocks, the ordering of the transactions is fair.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

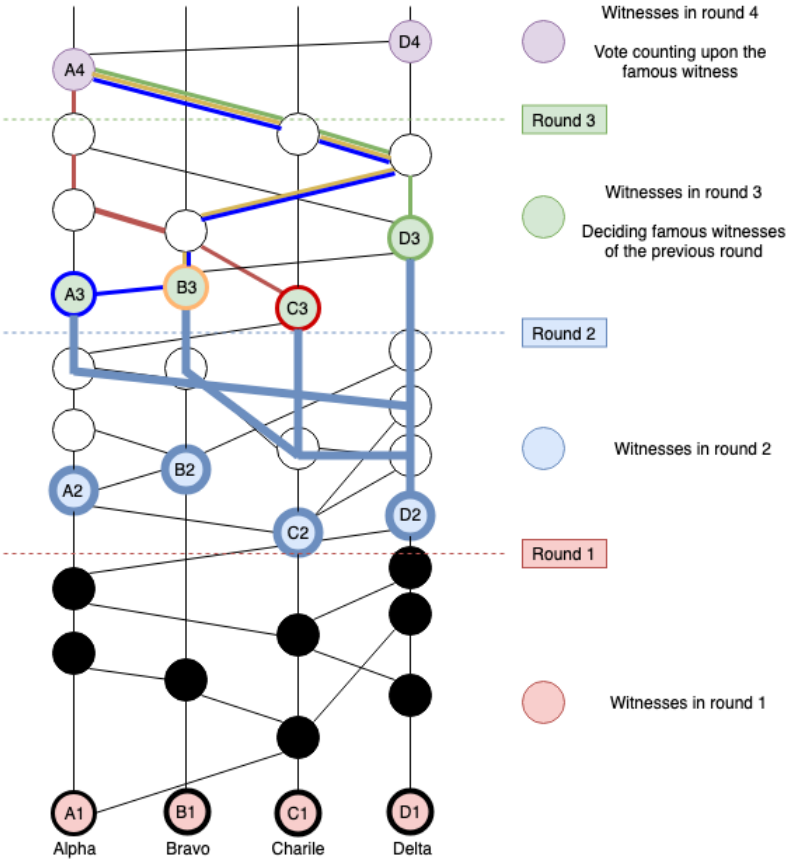

Figure 1. Hashgraph and the consensus algorithm.

In Figure 1, each circle is an event, containing the digital signature of the node that has created it, transactions, the consensus timestamp when the event was created, the hash of the node's previous event and the hash of the received event.

To explain how the Hashgraph works, witnesses are the first event of a node in a round, and a new round starts whenever witnesses are seen by a majority of the nodes. A witness is famous whenever more than a third of the nodes have received this event at the start of the next round. Figure 1 shows a sequence of rounds in which D2 is decided as a famous witness by A4, meaning that every previous event, tracing back from D2, will reach finality. D2 can be seen by A3 through the previous Alpha event and the event which was gossiped by Delta. By B3, D2 is seen through Bravo's previous event, Charlie's event and Delta's event, which were all gossiped to Bravo. C3 can see D2 through its own previous event, which was gossiped by Delta. Thus, each node has a gossiped event by which it can trace back to D2 and declare it a famous witness. Using the same principle of tracing back to each previous witness through a majority of the next witnesses, we can draw the conclusion that each node in round 2 is a famous witness.

As to this point, the famous witnesses are decided for each node, but they still need to see what each of them has decided, and the vote counting is done in the fourth round, where witnesses from the third round need to be 'strongly seen' by witnesses in the next round; this means that it is not enough for a node to see its previous witness, so it needs to see it through events of the majority of nodes, which means two thirds of the nodes or by a supermajority of the nodes, considering their stakes in the virtual voting. As such, A4 can decide upon the famous witnesses in the second round, by seeing the witnesses in the third round through a majority of nodes, A4 can see A3 through A, C, D and B, B3 through A, C and D and B, C3 through A, B and C and D3 through A, C and D.

After A4 has decided on the famous witnesses, it can safely confirm the events marked in black, as they have been seen by all the famous witnesses and thus consensus has been reached for all the black events. If it was to take into consideration the fifth round, the events in round 2 would start to

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

be confirmed with the possibility that not all events in round 2 will be confirmed in the fifth round, as not all witnesses need to be famous as in the situation described above.

It is mathematically proven that, despite every node and witness doing their own calculations, they will end up with the same result and the Hashgraph will look the same for all the nodes participating in the consensus [44].

Using the Hashgraph algorithm, the experiments realized by Hedera show that a very high volume of 100-bytes transactions per second reach finality in a short period of time. With a 3 seconds latency, when the network is spread across the globe in 8 regions, it reaches consensus finality in 3 seconds, when 32 computers are running 50.000 transactions per second [46].

Proxy staking is a way in which wallet owners can delegate their Hedera tokens, called HBars, to a node that participates in the consensus, contributing to that node's voting weight. By proxying their stakes, nodes are paid while their tokens are kept inside their wallets, without being deposited somewhere else or burned.

Mirror nodes are another way in which a user will be able to receive micro-payments and it will be available for everyone since the start of the mainnet. To keep the network as lightweight as possible, mirror nodes will be the only ones containing a full history of the transactions, while not participating in the consensus. Mirror nodes can be pinged or subscribed to, as a means through which users can receive information about transactions, smart contracts or the file storage, by paying a small fee.

Hedera Hashgraph is a fee-based system, where all their services, transactions and queries need to be paid through cryptocurrency micro-transactions. Every transaction will be sent to one single node in the network and will contain multiple fees:

- a fee for the whole network, that has to be shared with the consensus participants,
- a node fee, given to the node addressed, to afterwards receive the confirmation receipt, and
- a service fee, if any smart contracts or file storage service have been requested to work with.

Additionally, users will have to pay for their node to be available on the network.

With all this being said, it will be a strong incentive for everyone to participate in the consensus through proxy staking as, by this means, they could earn back part of the fees they paid to live and use the network.

Hedera Hashgraph is in its infancy, with test phases being run on its mainnet by a limited group of individuals, who have done KYC and AML checks, and have been given the opportunity to join the community.

Like all the DLTs, Hedera is also prone for a cold start. When a malicious node can be one of the early adopters, it can have the opportunity to take over the network rather easily. That is why the platform has set up different control mechanisms, such as the Hedera Treasury, which contains 65% of the HBars, which are being staked to a governing council. Part of the governing council was already announced and will eventually consist of 39 organizations, including IBM, Deutsche Telekom or Swisscom, coming from 18 different fields [47]. Its diversity, with companies from various industries spread throughout the globe in 10 major regions, assures that Hedera Hashgraph will become a general-purpose public ledger [48]. Each member has a limited stay inside the council, which consists of maximum 2 terms of 3 years, and which has a weight in the decision making for growing Hedera. In the first years of the mainnet, we will see nodes of each member of the governing council participating in the consensus mechanism, with other members being able to join the consensus only through proxy staking. This way, with the legal and technical controls put into place, the network will never fork, taking into consideration that, in time, it will be made up of millions of users with no possible way of a byzantine node to own one third of the network, opening itself more to becoming a truly distributed ledger.

With all the novelty features, the smart contracts, file storage support and the economic system provided by the Hedera Hahgraph, many projects started to be developed. Hedera has been participating in events, creating workshops and webinars, organizing hackathons and the Helix

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

incubator, and has managed to bring new functionalities and applications by launching the main network in September 2019. Projects developed during the hackathons and in the Helix incubator have stood out with many new use-cases. Here we name a few projects participating in the incubator or community driven dApps [49]:

- Paypar or Payable Links is an API which enables web pages to be accessed only after paying a small fee;
- HopOn enables a way of sharing mobile data by paying a small fee decided by the service provider;
- Hashing Systems, similar to the Ethereum Name Service, will allow Hedera wallets to be easily identified;
- Hash-Hash is a community website which lists all the wallets and their balances inside the Hedera Network.

There are hundreds of dapps in development, a few of them in advanced stages, in fields like media, real estate, insurance, gaming, privacy and personal data sharing, supply chain or social media.

The interface for building on top of the Hedera Hashgraph is delivered by using Protocol Buffers 'protobufs' and gRPC, providing a performant interaction between the nodes and the client. While protobuf is language-neutral, gRPC offers support for 10 different languages, making the Hedera Hashgraph usable on any kind of device and application. Hedera currently has SDKs developed in C, Go, Java, Python and Rust with SDKs to support other programming languages, like NodeJS, which started being developed by the community.

With all the great advancements, Hedera Hashgraph turns out to be one of the best options available, with a big community already by their side. Although compared to Bitcoin or Ethereum, Hedera Hashgraph is not yet open-source, so we cannot have a deep understanding of the underlying code, this might change in the future, but keeping in mind that the Hashgraph is a patented algorithm, nobody else will be able to use it without permission. The Solidity smart contracts support is twofold as well, on one side different decentralized apps can be brought from Ethereum with ease, which will help the network grow faster, on the other side, being a programming language designed for Ethereum, some variables like block properties or gas in Solidity do not exist for this platform.

Comparing Ethereum and Hedera, we can note the following conclusions:

- there are more transactions and no forks on Hedera;
- history is not entirely saved on the nodes on hashgraph, instead only some of the latest transactions are stored, which are needed for the virtual voting consensus mechanism;
- on Ethereum it is paid for changing the state and interrogating is free, while on Hedera there are small fees for everything, for the account or for smart contracts to be available;
- everyone can participate in the consensus with Hedera by proxy staking, which can earn you the money for paying the fees;
- there is a possibility for 34% attack on Hedera, while the percentage is 51% on Ethereum, so attacks can happen on Hedera if you control a smaller percentage of votes;
- both can run Solidity smart contracts, on Hedera there is the possibility to store files on the hashgraph with a certain fee, based on size and time of availability, while with Ethereum you can store on IPFS, which may sometimes be too slow.

4.3. Second layer protocols - the Hashed Timelock Contracts

While many developers in the community are trying to find new ways to solve the limitations of the blockchain by creating new protocols, some have started shifting their focus on solutions on a second layer off-chain protocol to fix the problems of Bitcoin and Ethereum, along with other DLTs [50]. These off-chain established channels between users are interesting as they offer new solutions

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

for improving inter alia, the scalability, in exchange for the security the blockchain can offer. A drawback is that these networks haven't proved to be secure and are prone to DDoS and other cyberattacks, which can take nodes inside the network offline, a fact already happened to the Lightning Network [51].

With Bitcoin and Ethereum being the pioneers of designing such networks based on Hashed Timelock Contracts, the network has also been tested to work interoperable with other cryptocurrencies, thus opening the path to Decentralized Exchanges (DEX) through Atomic Swaps and Submarine Swaps. This process will cut out the single point of failure from today's cryptocurrency exchanges and will make the entry points to the electronic cash systems more secure.

Hashed Timelock Contracts (HTLCs) have been created to securely make bidirectional transfers across a network of channels, where transfers need to make it across multiple trustless nodes in order to reach their final destination [52].

Raiden is an off-chain network which allows ERC20-compliant tokens to be transferred on the Ethereum blockchain [53], using payment channels established through a Hashed Timelock Contract (HTLC). By using these payment channels, the only transactions made on-chain are those establishing and closing a payment channel between 2 parties. Between these 2 on-chain transactions, any number of token exchanges can be made between the involved parties, as long as there is enough liquidity available on the payment channel, with minimal transaction fees and at a very high speed.

Plasma Network is a framework proposed in a paper written in collaboration by Joseph Poon, co-author of the Lightning Network, and Vitalik Buterin, the creator of Ethereum [54]. Plasma proposes to scale smart contracts by moving state transitions on nested layers of the blockchain, lifting heavy computations off the main chain, while enforcing to it through fraud proof mechanisms. The network is created by building Plasma Contracts on top of the main blockchain, enabling token creators to have their own nested blockchain, which takes care of the high computations, posting only a hash and associated data on the main chain for every block, instead of the high volume of computations [55]. It uses smart contracts which allow fraud proofs to be posted on the main chain if any malicious activity happens on the last block. If that happens, the block is declared invalid and it is rolled back, while the block creator is then penalized. One of the unique features of Plasma is that it allows the private blockchain to run and get the root hash validated inside a public blockchain, which ensures security and other benefits of the public blockchain, thus creating a trustful and flexible environment for small companies to run in a market of huge multi-industry corporations.

Another off-chainnetwork is Trinity, designed for Neo; it aims to build HTLC on top of it, similar to Raiden or the Lightning Network, providing smaller fees, while increasing the transaction throughput [56].

4.4. The Lightning Network

In 2013, with the limitations of Bitcoin, the community started to elaborate on Satoshi Nakamoto's idea of using time locks and multisig to change unrecorded transactions in an email exchange [57]. In 2015, Joseph Poon and Thaddeus Dryja published the whitepaper of the Lightning Network [36], a second layer network built on top of Bitcoin, that would enable the blockchain to scale to billions of transactions per second.

The Network is the most evolved off-chain scaling solution with three companies working on it in different programming languages. ACINQ is working on a Scala implementation and they are the first to have delivered a Mobile Lightning Wallet called Eclair. Blockstream is working on C-Lightning, written in C programming language, and Lightning Labs is working in Golang on the Lightning Network Daemon (lnd).

There have been many successful tests for sending real bitcoin with the implementations of all the three companies. This not only shows that the Lightning Network is working, but also the interoperability between implementations. The development process is following a set of rules called "Basics of Lightning Network" (BOLTs). With the help of the BOLT structure, the teams manage to work independently and developers will be able to write implementations in any programming language, while keeping them interoperable.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

While the network has been designed to scale public blockchains, it also offers interoperability between blockchains, privacy between the parties involved in a payment channel in terms of the transfer destination and new types of smart contracts. These can empower the limitations of Bitcoin, as well as the ability to run decentralized exchanges on top of it. On the other hand, payment channels are run by a single computer inside the network, which creates a more vulnerable environment.

Privacy is achieved on the Lightning Network by the source-based onion routing, where the transfer is done through multiple hops, in order to reach the final destination, where each node can only see the next hop addresses. The node wanting to establish a channel creates several paths based on the information it receives about channel fees, capacity of the channels, and encrypts each hop based on the nodes' public keys. With the path's encrypted layers, each node in the route can decrypt the outer layer by using its private key, figuring out the successor node's address, to which it needs to pass the information in order to get closer to the destination.

The Network is based on HTLC, that can be created by using the Bitcoin scripting language, which is not Turing complete and can also be extended to other smart contract enabled platforms, such as Ethereum, Litecoin, Ripple and ZCash among others.

Fees will be so small that users won't even notice them. On the Lightning Network, the smallest micro-transaction which was successfully made values at $0.000000037 [58]. With such a small value, the user will certainly overlook the payment fee, as thus he will access a genuine piece of information. With the subscription business models used by big players nowadays, a solution with pay-per-view articles or pay-per-minute videos will likely be embraced by the communities.

Currently, the technology isn't ready for an official release as there are still many bugs to fix, but the network runs on testnet and mainnet. With the help of [59] we could see that in September 2019 there were 10,000 nodes running inside the network. Channels can be refunded through wallets.

By holding a well-funded hub on the Lightning Network, it can help earning more fees by being available for more payment channels. While this is considered to make the network more centralized, the hubs can become a target to hackers, which makes this not a feasible solution.

5. Discussions and Conclusions

Decentralized Ledger Technologies are one of the fastest evolving technologies, with many promising solutions being developed. In this paper, we have presented extended reviews of four complementary technologies for blockchain, the first in the form of DAGs, a variant being Hedera Hashgraph, which have gained the attention and have been adopted by many leading organizations. Also, we have talked about new second-layer protocols, that are being developed for the main public blockchains, Bitcoin and Ethereum, and which can be scaled to most of the available DLTs.

The following table summarizes the way the technologies presented in the article respond with novel concepts to the blockchain trilemma challenges and also other performant particularities they offer (marked with a plus sign), but also some drawbacks (marked with a minus sign).

Table 1. Addressing blockchain trilemma issues.

Technology	Blockchain Trilemma issues	Notes
Directed Acyclic Graphs	• because the nodes (users) validate the transactions, the more transactions and users are, the faster the confirmations are;	• accommodate new consensus mechanisms, reducing the energy consumption of PoW (+); • some implementations can run on mobile devices (+); • being in an experimental state, they still have to prove their security (-); • partial centralized (-);

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 October 2019 doi:10.20944/preprints201910.0071.v1

Hedera Hashgraph	• for this type of DAG, gossip-about-gossip with virtual voting algorithm allows every member of the network to be part of the consensus through proxy staking; • the specific consensus and reduces the communication overhead; • efficiency in bandwidth usage as only information about transactions are transmitted;	• an efficient consensus mechanism that makes transactions reach finality very fast (+); • fairness concept: keeping the time and order of transactions fair, with no security tradeoffs (+); • innovation in many domains, micro-payments (+); • prone for a cold start: if a malicious node is one of the early adopters, it can take over the network rather easily (-); • it is a patented technology, not an open-source project (-);
Hashed Timelock Contracts	• tested to work interoperable with other cryptocurrencies, thus opening the path to Decentralized Exchanges (DEX) through Atomic Swaps and Submarine Swaps;	• between two on-chain transactions, any number of token exchanges can be made as long as there is enough liquidity available on the payment channel, with minimal transaction fees and at a very high speed (+); • haven't proved to be secure and are prone to DDoS and other cyberattacks (-);
The Lightning Network	• is a second layer network built on top of Bitcoin, being the most evolved off-chain scaling solution, that would enable the blockchain to scale to billions of transactions per second; • interoperability between implementations, as the development process is following a set of rules called "Basics of Lightning Network" (BOLTs);	• the technology isn't ready for an official release as there are still many bugs to fix, but the network runs on testnet and mainnet (-);

With developers working for on-chain and off-chain solutions and with new DLTs being developed, we will soon see solutions fitting most of the use-cases.

In order for the blockchain to work at scale, blockchain solutions should be integrated in proven, successful solutions, where DLTs are integrated with the off-chain in interoperable infrastructures.

The blockchain community should integrate DAOs, in which blockchain is used as a means to govern the workflow and should set up a solution to benefit the decentralized ledger in order for other entities to gain trust in adopting this technology.

With the ongoing progress and with most of the top companies studying the DLT ecosystem and the ways to make it work for them, education needs to become a major concern. Not only individuals need to understand the true benefits of blockchain, but also the education needs to shape up new engineers to help in analysing, designing and developing the future of the internet of value, while making use of all the available technologies.

Many people do not understand the differences between the blockchain and Bitcoin, with Bitcoin and cryptocurrencies being only one of the use-cases of the blockchain, and what the benefits of the blockchain technology are. More specific training programs and adaptation of university curricula are needed.

As it is difficult for a single solution to achieve the perfect balance of scalability, interoperativity and sustainability, the evolution of DLTs is becoming more interesting as each platform comes with a specific approach to the blockchain trilemma.

We appreciate that Directed Acyclic Graphs (DAGs) could represent the future for public permissionless distributed ledger technologies, while the blockchain can continue to work on permissioned private DLTs.

Author Contributions: Methodology, Victor Holotescu and Radu Vasiu; Project administration, Victor Holotescu; Resources, Victor Holotescu and Radu Vasiu; Supervision, Radu Vasiu; Validation, Radu Vasiu; Writing – original draft, Victor Holotescu; Writing – review & editing, Victor Holotescu and Radu Vasiu.

References

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
2. Deshpande, Advait, Katherine Stewart, Louise Lepetit, and Salil Gunashekar. "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards." Overview report The British Standards Institution (BSI), 2017.
3. D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," in *Advances in Cryptology — CRYPTO' 88*, 1990, pp. 319–327.
4. "CoinDesk ICO Tracker - CoinDesk." [Online]. Available: https://www.coindesk.com/ico-tracker. [Accessed: 04-Apr-2019].
5. "EU launches blockchain association to accelerate distributed ledger technology adoption | VentureBeat." [Online]. Available: https://venturebeat.com/2019/04/03/eu-launches-blockchain-association-to-accelerate-distributed-ledger-technology-adoption. [Accessed: 04-Apr-2019].
6. "18 Blockchain Consortia You Should Know About – Blockchain Blog – Medium." [Online]. Available: https://medium.com/blockchain-blog/18-blockchain-consortia-you-should-know-about-6262b6a30ba9. [Accessed: 04-Apr-2019].
7. "MIT Digital Currency Initiative." [Online]. Available: https://dci.mit.edu/. [Accessed: 04-Apr-2019].
8. "EUBlockchain | An initiative of the European Commission." [Online]. Available: https://www.eublockchainforum.eu/. [Accessed: 04-Apr-2019].
9. Ometoruwa, T, "Solving the Blockchain Trilemma: Decentralization, Security & Scalability", *Coinbureau*, 2018. [Online]. Available: https://www.coinbureau.com/analysis/solving-blockchain-trilemma. [Accessed: 29-May-2019].
10. Croman, Kyle, et al. "On scaling decentralized blockchains." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016.
11. M. Rauchs *et al.*, "Distributed Ledger Technology Systems: A Conceptual Framework," *SSRN Electron. J.*, 2018.
12. F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. Inform.*, vol. 36, pp. 55–81, Mar. 2019.
13. M. Dabbagh, M. Sookhak, and N. S. Safa, "The Evolution of Blockchain: A Bibliometric Study," *IEEE Access*, vol. 7, pp. 19212–19221, 2019.
14. D. Chaum, "Blind Signatures for Untraceable Payments," in *Advances in Cryptology*, 1983, pp. 199–203.
15. Dai, Wei. "B-money proposal." White Paper, 1998.
16. Szabo, Nick. "Bit gold", 2005. [Online] Available: http://unenumerated.blogspot.com/2005/12/bit-gold.html.
17. Sander, Tomas, and Amnon Ta-Shma. "Auditable, anonymous electronic cash." In Annual International Cryptology Conference, pp. 555-572. Springer, Berlin, Heidelberg, 1999.
18. Chohan, Usman W. "A history of bitcoin.", 2017. [Online]. Available at https://ssrn.com/abstract=3047875.
19. Tom Lyons, Ludovic Courcelas, Ken Timsit, "Blockchain for government and public services", 2018. [Online]. Available: https://www.eublockchainforum.eu/reports.
20. L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst. TOPLAS*, vol. 4, no. 3, pp. 382–401, 1982.
21. D. A. Baliga, "Understanding Blockchain Consensus Models," 2017.
22. G. Konstantopoulos, "Understanding Blockchain Fundamentals, Part 3: Delegated Proof of Stake," *Medium*, 11-Jun-2018.
23. Buterin, Vitalik, Tweets on Blockchain Trilemma, in "Vitalik Buterin And Nouriel Roubini Discuss Blockchain Trilemma, Moderated Debate To Come?", Putney, Dani, 2018. [Online] Available at https://www.ethnews.com/vitalik-buterin-and-nouriel-roubini-discuss-blockchain-trilemma-moderated-debate-to-come.
24. Tom Lyons, Ludovic Courcelas, Ken Timsit, " Scalability, Interoperability and Sustainability of Blockchains", 2018. [Online]. Available: https://www.eublockchainforum.eu/reports.

25. Bashir, Imran, "Mastering blockchain: Distributed ledger technology, decentralization, and smart contracts explained", Packt Publishing Ltd, 2018.
26. V. Zamfir, "The History of Casper — Part 1," *Vlad Zamfir*, 07-Dec-2016.
27. CoinLore, "Cryptocurrrency List", 2019. [Online]. Available: https://www.coinlore.com/all_coins.
28. D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8202, Oct. 2018.
29. T. Hardjono, A. Lipton, and A. Pentland, "Towards a Design Philosophy for Interoperable Blockchain Systems," *ArXiv180505934 Cs*, May 2018.
30. A. Lipton and T. H. S. Pentland, "Digital Trade Coin (DTC): Towards a more stable digital currency," p. 18.
31. "Blockchain Size," *Blockchain.com*. [Online]. Available: https://www.blockchain.com/charts/blocks-size. [Accessed: 30-Sept-2019].
32. "Ethereum Sync (Archive) Chart." [Online]. Available: https://etherscan.io/chartsync/chainarchive. [Accessed: 30-Sept-2019].
33. "Hashrate Distributie," *Blockchain.com*. [Online]. Available: https://www.blockchain.com/pools. [Accessed: 08-Apr-2019].
34. "Bitcoin Energy Consumption Index," *Digiconomist*. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Accessed: 11-Apr-2019].
35. "Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?," *HowMuch*. [Online]. Available: https://howmuch.net/articles/crypto-transaction-speeds-compared. [Accessed: 26-Mar-2019].
36. T. E. Jedusor, *Mimblewimble*. July, 2016.
37. Wheeler, Zach, "Beam Vs Grin: Who's Nimble At Mimblewimble?", 2019. [Online] Available: https://ec.europa.eu/digital-single-market/en/policies/76023/76123.
38. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.
39. El Ioini, Nabil, and Claus Pahl. "A review of distributed ledger technologies." In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pp. 277-288. Springer, Cham, 2018.
40. S. Popov, "The tangle," *Cit On*, p. 131, 2016.
41. Q. Bramas, "The Stability and the Security of the Tangle," Apr-2018.
42. Churyumov, Anton, "Byteball: A decentralized system for storage and transfer of value.", 2016. [Online]. Available: https://obyte.org/Byteball.pdf
43. Holographic storage for distributed applications -- a validating monotonic DHT "backed" by authoritative hashchains for data provenance (a Ceptr sub-project): holochain/holochain-proto. Holochain, 2019.
44. Baird, Leemon, "The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance" Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep., 2016. [Online]. Available: https://www.hedera.com/hh-whitepaper-v1.5-190219.pdf.
45. "Welcome! | The Coq Proof Assistant." [Online]. Available: https://coq.inria.fr/. [Accessed: 08-May-2019].
46. Baird, Leemon, Mance Harmon, and Paul Madsen. "Hedera: A Public Hashgraph Network & Governing Council", 2019. [Online]. Available: https://www.hedera.com/hh-whitepaper-v1.5-190219.pdf.
47. H. Hashgraph, "Council," *Hedera Hashgraph*, 06-May-2019. [Online]. Available: http://www.hedera.com/council. [Accessed: 06-May-2019].
48. H. H. Team, "Hedera Hashgraph Announces Initial Group of Governing Council Members," *Medium*, 20-Feb-2019.
49. Hedera. "Hedera Hashgraph Announces Winners Of Global Hackathon And Hedera MVPs", Medium, 2018. [Online] Available: https://medium.com/hashgraph/hedera-hashgraph-announces-winners-of-global-hackathon-hedera-mvps-c43df7f30c08.
50. T. C. Oracle, "The Current vs Future State of Distributed Ledger Technology," *Noteworthy - The Journal Blog*, 30-Apr-2019. [Online]. Available: https://blog.usejournal.com/the-current-vs-future-state-of-distributed-ledger-technology-e146d90a3099. [Accessed: 05-May-2019].
51. M. H. Miraz and D. C. Donald, "LApps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications," p. 6.
52. J. Poon and T. Dryja, "The Bitcoin Lightning Network:," p. 59.
53. "Raiden Network." [Online]. Available: https://raiden.network/. [Accessed: 12-May-2019].
54. J. Poon and V. Buterin, "Plasma: Scalable Autonomous Smart Contracts," p. 47.

55. "(1) De/2018 - Cryptoeconomic Incentive Mechanisms - Joseph Poon, Plasma & Lightning Network - YouTube." [Online]. Available: https://www.youtube.com/watch?v=6kv0DTU3T_E. [Accessed: 12-May-2019].
56. "Trinity." [Online]. Available: https://trinity.tech/#/writepaper. [Accessed: 12-May-2019].
57. M. Hearn, "[Bitcoin-development] Anti DoS for tx replacement," 17-Apr-2013.
58. "Lightning Network Milestone: 'Micro-Auction' Art Piece Sells for $0.000000037," *Bitcoinist.com*, 21-Dec-2018. [Online]. Available: https://bitcoinist.com/lightning-network-black-swan-cryptograffiti/. [Accessed: 06-May-2019].
59. "1ML - Lightning Network Search and Analysis Engine - mainnet." [Online]. Available: https://1ml.com/. [Accessed: 30-Sept-2019].