Distributed Ledger Technologies: A Review of Advancements and Milestones

By

Naman R Bhardwaj

Student, Department of Information Technology, Dr Akhilesh das Gupta Institute of Technology and Management, New Delhi, India

Abstract

The goal of distributed ledger technology (DLT) is to achieve a trustless, decentralised and distributed storage of transactions which is synchronised across multiple sites, devices and geographical locations which, in turn, would make it immutable and dependable. Such a ledger can solve a multitude of issues in financing and record-keeping and therefore it has now become a popular field of research in the past few years.

Although blockchain is the most prominent and well known DLT, there are newer kinds of DLTs as well. These are: Directed Acyclic Graph (DAG), Hashgraph, Holochain and Radix.

In this study, we review the various DLTs and how they have improved over the years, and also the feasibility of them replacing the current record-keeping technologies.

Keywords: distributed, decentralized, blockchain, consensus, permission,

Introduction

A distributed ledger is described as a decentralised, distributed and trustless ledger which makes it dependable, immutable, synchronised and openly available to the users of that distributed ledger. The meaning behind these words is as follows:

- Decentralised: There is no central body that governs the working of the ledger, nor has the authority to alter it.
- Distributed: The ledger is spread across the multiple members(computers), which are called nodes, and every node has the same authority.
- Trustless: None of the parties registering transactions on the ledger have to trust one another, they simply trust the DLT itself to identify malicious transactions from the rest.

It is these properties that justify the importance and existence of DLTs. Such ledgers can prove indispensable for almost every sector that requires keeping a record of any and all kinds of transactions. This versatility is what makes this new field progress so fast.

DLTs gained serious traction ever since Satoshi Nakamoto mined the genesis block (or 0th block) of his blockchain Bitcoin[1] in 2009. This event was of paramount significance since it was the first working implementation of DLT which had solved the double-spending problem and arguably the first cryptocurrency that really mattered. It marked the beginning of the era of cryptocurrencies and since then, a multitude of innovations in the DLT front have taken place thanks to the momentum Bitcoin[1] managed to surmount.

But, the first idea of distributed trust can be credited to Stuart Haber and W. Scott Stornetta for their work on “How to Time-Stamp a Digital Document[2] “, 1991, in which they tackle the issue of trust against the tampering of digital documents and mentions the use of collision-free hash, digital signatures and Two Time Stamping Schemes[2] along with a distributed network of users to tackle the issue, which is the idea blockchain and DLTs are based upon.

After more than 10 years, in 2002, David Mazières along with Dennis Shasha went deeper with the concept, studying how data can be stored in a block format. In their paper "Building secure file systems out of Byzantine storage[3]", their focus was on data structures and protocols of a multi-user network file system called SUNDR[3] (Secure Untrusted Data Repository). This file system highlighted blockchain's ability to store data in blocks, thus providing the foundation for today's blockchain applications.

The primary challenges for a DLT are Byzantine Generals Problem[4] (BGP) and the double-spending problem.

Byzantine Generals Problem[4] basically points out that the participants involved in transactions may or may not be malicious and as such, the participants agreeing upon a transaction in order to verify it requires some consensus mechanisms in DLTs so that only the legitimate transactions are added to the ledger. There are many kinds of consensus mechanisms out there and many more are being researched as well.

As for the double-spending problem, the ledger itself is publicized and available to all, so it is remedied. Basically, all transactions become known by everyone and so false transactions will be easily identified based on the time stamps.

Now, let us start reviewing the DLTs.

1. Blockchain:

A blockchain is a DLT which collects transactions into a block, assigns it a number, a hash and a timestamp, and it gets verified by consensus mechanism. Once a transaction block is verified, it is added to the end of the chain of blocks that already exists and every node receives a copy of it. Also, a Merkle Tree of hashes for every block is maintained. This way, if a node tries to alter any transaction in any block, the whole chain collapses for that node and the attack becomes useless.

These days, however, 51% attacks have been happening with certain blockchains which use Proof of Work, which basically hijack the new block consensus process and can give the blockchain any direction they want.

The downside of blockchain mainly is the scalability issue, which refers to the limited ability of blockchains to process transactions as so many steps are involved.

The various consensus mechanisms used by blockchains are:

- Proof of Work[12]: In this, participants called miners 'mine' for adding the next block of transactions to the existing chain. Essentially, they compete to solve a series of computations and the first one to complete gets to add the block to the chain, and is compensated for it with some Bitcoin, called the miner's fees.
- Proof of Stake[11]: In this consensus algorithm, a random participant is chosen to validate the next block, and the chances get better the more cryptocurrency of that blockchain the participant has. So, the participant with most cryptocurrency at the moment would have the most chance to validate the next block.
- RAFT[9]: In this algorithm, a 'leader' of the cluster is elected by nodes to complete client requests and sends the transaction data to other servers to maintain synchronization by duplicating the logs of the current server. To prevent repetition, only one entry for an index is permitted in every server.
- Proof of Elapsed Time[10]: In this algorithm, basically all nodes must wait

for a randomly calculated period of time and whichever succeeds can add the block to the chain.

- Practical Byzantine Fault Tolerance [8] which is a revolutionary algorithm that has Byzantine Fault Tolerance and works as long as less than ⅓ of the nodes are malicious.

There are many more consensus algorithms

The most popular blockchains as of now are Bitcoin, Ethereum, and the Hyperledger project's Fabric and Sabretooth.

Bitcoin:

Blockchain is like the progenitor of DLTs, as it was the first one to be successfully implemented in 2009 by S Nakamoto in the form of the Bitcoin [1] blockchain.

The consensus mechanism it uses is Proof of Work.
It is a permissionless blockchain, in the sense that there is no single entity that can accept or reject transactions.

This way, miners are incentivized and motivated to keep the mining going, allowing the blockchain to sustain.

But the downsides of this consensus method is its high global power consumption and its slow speed to verify transactions, which for Bitcoin is about 6 transactions per second (for reference, VISA handles 1700 tps).

This blockchain, however, was a proof of concept for the many blockchains that were about to follow it.

Ethereum:

The Ethereum [5] blockchain came into play in late 2013-2014 as a cryptocurrency and decentralized applications platform. It revolutionized blockchain technology by introducing Smart Contracts [5], which functioned as an autonomous set of regulations to govern transactions and so allowed the transactions to be bound by formal contracts if needed be. This opened new doors for the technology as now one could rely on Ethereum itself to uphold the set of laws previously agreed upon by the parties involved. The reliability of automated transactions had never been higher.

These Smart Contracts also opened the path to decentralized applications, which are applications existing on the blockchain itself and ran on the Ethereum Virtual Machine embedded into the chain. This allowed to not only make transactions reliable and autonomous but also to create environments in which the participants could engage in trades, or voting and transfer of data via payloads attached to transactions and so much more.

Ethereum currently works with Proof of Work mechanism (allowing 15 transactions per second), but Ethereum 2.0 which is an upcoming hard fork in the chain, would change the consensus mechanism to Proof of Stake [11], which is expected to greatly increase the speed to about 100000 transactions per second.

The Ethereum 2.0 is currently in testing stage and the release date is said to be November 2020.

Hyperledger Fabric:

The Hyperledger project is an umbrella project of open source blockchain technologies and any related tools which was initiated in December 2015 by the Linux Foundation. Its prominent blockchain framework Fabric is a widely used permissioned blockchain framework, which is made to be used in closed environments like corporate organisations and more. This blockchain is made to fit the requirements of one's corporation to create a distributed ledger to keep complete records of everything.

Unlike the previous examples, there is no linked cryptocurrency with it, as it was not made for such a purpose.

The USP of Hyperledger Fabric [6] is its modular structure, which can be plugged with many application programming interfaces(APIs) , its support for distributed applications, its plug and play nature of customizable modules and the fact that it is open-source.

Rather than smart contracts of Ethereum which require fee to run, Fabric utilizes Chaincode[6] which is built into the chain itself for its distributed application support.

These features have attracted many tech giants towards itself and this umbrella project is now bigger than ever.

The consensus algorithm generally used in Hyperledger Fabric [6] is RAFT[9] which allow swift functioning for the blockchain (~2000 transactions per second).

Hyperledger Sawtooth:

Hyperledger Sawtooth[7] is another part of Hyperledger project in which permissioned and permissionless blockchains can be created using this framework. It is familiar to Fabric in sense that it is also modular and supports a multitude of cloud services and APIs.

The smart contract alternative used in Sawtooth is called Transaction Families [7] in which the application data, transferring data and transaction data are separated but encapsulated into one and can be installed in the blockchain or on-chain like smart contracts.
The consensus algorithms which can be used in it are: Proof of Elapsed Time [10], Practical Byzantine Fault Tolerance [8] and RAFT [9] among others which grant it a speed of about 1000 transactions per second. Again, there is no cryptocurrency assigned with it.

2. Directed Acyclic Graph:

The structure of DLT used here is that of a directed acyclic graph of transactions in which newer transactions verify the older ones using consensus algorithms in a random order and if they are able to verify those older transactions, only then the newer transaction joins the older ones.
Here, joining means for the newer node to have the hashes of the older nodes and subnodes it is connecting to.Since only a meagre number of algorithms are verified per user at a time, the transaction speeds are much faster than conventional blockchains. One of the main downsides, though, is that the confirmation or trust of the transaction depends on the depth of the transaction, i.e., how many transactions have joined that transaction, and its sub-adjacent transactions and so forth. So, a transaction may never achieve 100% confirmation, but that does not mean it is not trustworthy.

The scalability is not much of an issue for DAG as a node simply does its part if it wishes to publish a transaction here.

NXT:

In this category, NXT is an exception. It does not form a DAG of transactions, but a DAG of blocks of transactions.
In NXT [13], a block of transactions is generated every 60 seconds, and by Proof of Stake method, a miner is chosen to add the block to the DAG, connecting it to two random blocks and so on.
A block is considered verified if it has a depth of 10 blocks after it.
In combination with Proof of Stake, the older the coins are, the more is their value. This way, it results in a more Proof of Stake model.

Since this project was started by an anonymous developer and is open- source, it is now mainly managed by the community.

As of the current version of NXT, there is no smart contract support. But it is expected to come eventually.
The transaction speed is about 4 per second.

This is the first DAG based DLT and paved way for the rest.

IOTA Tangle:

In IOTA Tangle[14], the transactions form a DAG and the peers who add a new transaction verify two transactions with zero depth, called tips, at random using Proof of Work consensus theorem and if they are authenticated successfully, then the new transaction attaches to those two older ones. The depth (distance from tips) is the indicator of the reliability of a transaction here.

For this DLT, there are no costs to carry out a transaction involved, as the work done by a participant to add a transaction is very meagre.

Since there are no transaction fees and supports smart contracts, this DLT fully supports zero-fee transactions, i.e., data transactions. This is by design as the agenda behind IOTA Tangle is to develop a DLT for Internet of Things devices, so that a fully self-sufficient machine economy can be created between the devices to enable a completely automated manufacturing/development environment.

One of the special features of IOTA Tangle is the ability to maintain an offline DAG as a concurrent transaction and upload at once to the Tangle. This allows for relevant transactions to be grouped together even when joined to the Tangle and more importantly, the IoT machine economy previously discussed can exist without the devices being connected to the internet by just being nodes of the same offline Tangle.

The transaction speeds depend on the number of participants that transact on the tangle. Roughly two years ago, the speed was 1 transaction per minute. But at this time, the transaction speeds are reaching 600-800 transactions per second.

OByte(formerly ByteBall):

OByte[15] is a DAG with a cryptocurrency called byte. The concept behind this is that the tokens can be exchanged for storing contracts, data and the transactions themselves on the DAG as nodes, with 1 token 'byte' corresponding to storing data of size of one byte.
This DLT was developed with the idea of building a tamper proof data storage to store data of transferable value like shares, currencies, property, debts, and the like.

The verification of transactions happens using 'witnesses' which are representatives chosen by the members of the DAG, and the longest chain of transactions which has transactions approved of by most witnesses, called main chain, form the verified transactions.
The transaction speeds for OByte currently are 10 transactions per second.

3.Hashgraph:

Hedera Hashgraph[16] by Swirlds is a data structure and consensus algorithm that stores the transactions in a graph-like structure, where every event or transaction is sorted in ascending order by time in the ledger which is shared between all the nodes.
This forms a DAG of transactions in the order of their timestamp, but this technology differs from the conventional DAG in the way that verification of transactions take place.
This DAG is proven to be Byzantine Fault Tolerant[16] and works on 'Gossip about Gossip' protocol. A gossip is a computer science algorithm in which one node calls one or more nodes at random and updates them about the transaction on that node. 'Gossip about Gossip' takes it one step further so that every transaction is gossiped about and every 'gossip' carries with it the parent hash and that of its parent and so on with it. This ensures

that every node ensures what one node knows about.
The verification process then becomes easier as the transactions that more people know about are verified first and double spending is prevented.

In Hashgraph, scalability is no longer an issue as nodes need not go through any bottlenecks and the consensus is rapid.

The transaction speeds reach upto 250000 transactions per second and Hashgraph currently only used as permissioned blockchain.

4. Holochain:

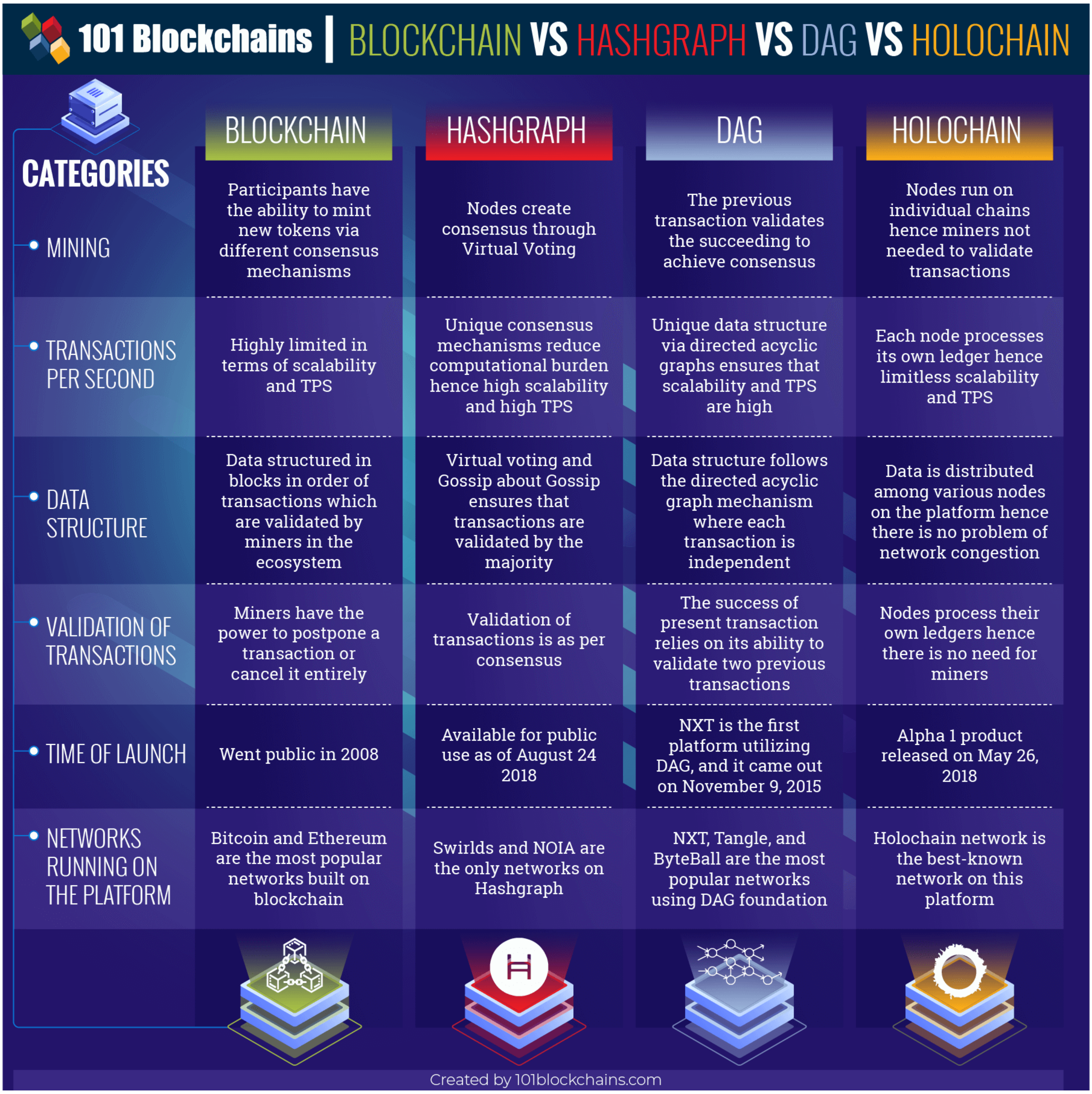
Holochain[17] is a distributed application platform on which every node can maintain their own hash chains(like blockchain). These are accessible by any node when they sync in with the Holochain and are digitally signed at the time of their origin.
The hash address of every node and the Dapps that they maintain on their personal hash chains is stored using a Distributed Hash Table (DHT) to allow navigation to the Dapps.

But, a node would eventually go offline, and to make the Dapp available during those times, one or more redundant copies of that application are copied to the nodes that visit the Dapp and their addresses are stored to the DHT as well.

As for validation of transactions, a distributed validation approach is used in Holochain. One must keep in mind that every node of Holochain is essentially running a Dapp on Holochain. Since every Dapp has their own set of validation rules (called DNA) , whenever a malicious user creates false transactions locally, they are essentially tampering with the Dapp that they are running locally. And since that Dapp would already have a reference in DHT, every node has access to its validation protocols. So, when a malicious node tries to enter its false transitions to the DHT, every node having the copy of that Dapp processes the transactions and if the DNA has been tampered with, the malicious node is identified by their signature on the transaction and is removed by the 'Immunesystem' protocol of Holochain along with their transactions.

This system allows for creation of secure Dapps on the Holochain platform.

Holochain uses a 'Proof of Service' consensus algorithm in which a node is rewarded based on the services provided by it to the other nodes. The reward is Holochain's cryptocurrency called Holo Fuel, which is then used to leverage services of other nodes in turn. This ensures a trusty environment. Since every node can maintain their own hash chain, there are no real limits to the transaction speeds and scalability of Holochain.



101 Blockchains | BLOCKCHAIN VS HASHGRAPH VS DAG VS HOLOCHAIN

CATEGORIES	BLOCKCHAIN	HASHGRAPH	DAG	HOLOCHAIN
MINING	Participants have the ability to mint new tokens via different consensus mechanisms	Nodes create consensus through Virtual Voting	The previous transaction validates the succeeding to achieve consensus	Nodes run on individual chains hence miners not needed to validate transactions
TRANSACTIONS PER SECOND	Highly limited in terms of scalability and TPS	Unique consensus mechanisms reduce computational burden hence high scalability and high TPS	Unique data structure via directed acyclic graphs ensures that scalability and TPS are high	Each node processes its own ledger hence limitless scalability and TPS
DATA STRUCTURE	Data structured in blocks in order of transactions which are validated by miners in the ecosystem	Virtual voting and Gossip about Gossip ensures that transactions are validated by the majority	Data structure follows the directed acyclic graph mechanism where each transaction is independent	Data is distributed among various nodes on the platform hence there is no problem of network congestion
VALIDATION OF TRANSACTIONS	Miners have the power to postpone a transaction or cancel it entirely	Validation of transactions is as per consensus	The success of present transaction relies on its ability to validate two previous transactions	Nodes process their own ledgers hence there is no need for miners
TIME OF LAUNCH	Went public in 2008	Available for public use as of August 24 2018	NXT is the first platform utilizing DAG, and it came out on November 9, 2015	Alpha 1 product released on May 26, 2018
NETWORKS RUNNING ON THE PLATFORM	Bitcoin and Ethereum are the most popular networks built on blockchain	Swirlds and NOIA are the only networks on Hashgraph	NXT, Tangle, and ByteBall are the most popular networks using DAG foundation	Holochain network is the best-known network on this platform

Created by 101blockchains.com

Source: https://101blockchains.com/blockchain-vs-hashgraph-vs-dag-vs-holochain/

5. Radix:

Radix[18] DLT is a platform for sole development of mainly DeFi(Decentralized Finance) applications, which is based on a sharded structure of 18.4 quintillion parts, each part assigned to an address for making requests or transactions and stores that data. This makes parallelism of transactions and consensus its strongest points which assist in scalability.

Its Radix Engine approach for programmability on the DLT allows for leveraging the sharded and easy to scale architecture for creating powerful Dapps easily by using state machine approach called Atom[20] model for running Dapps, which means that one could program the behaviour of their Dapp more precisely to result in a fixed state of the DLT after a particular operation takes place from a particular machine state.

Until February 2020, Radix used Tempo[20] DLT, which was successful in achieving about 1 million transaction per second, thanks to its sharded structure, and its unique consensus algorithm, in which related shards are grouped together around a root shard and a node serves groups of related shards at the same time. So, the more nodes serving a shard, the more is its verifiability. The nodes, of course, are compensated for serving the nodes this way.

However, as of March 2020, Radix has come out with its Cerberus[19] consensus algorithm as the Tempo algorithm could not guarantee the finality of a request, because it was a relaxed algorithm which allowed disagreements to exist on the DLT. Cerberus, however, uses Radix's very own Radix Engine's application layer to parallelize consensus. Each shard is assigned a consensus instance which begins working when called through the Radix Engine. To enable access to other shards during verification of request, a 'braiding' mechanism is put into place which connects and disconnects shards as and when required. This makes transactions atomic and allows for virtually unlimited parallelism.

This consensus model is expected to reach similar performance as that of the Tempo model, reaching about 1 million transactions per second without limits to scalability.

Although Radix is a new player, it has shown much promise and is in the spotlight for very appropriate reasons.

Conclusion

Just in the last decade, distributed ledger technologies have witnessed tremendous progress and the progress is only becoming more swift. It is a young field but with a great amount of applications and potential research. Although adoption of the technology is not widespread yet, many industry leaders are showing interest and studying the possibilities.

Outlook

While cryptocurrencies come and go, the FinTech industry is booming. Banks are adopting DLTs and many other esteemed companies are following suit. With such flexibility and innovation of DLT, it is no wonder that these events are taking place as we speak.

With all the work that is going into the field, it can be safely deemed that this technology is here to stay.

References

[1] Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* 4 (2008). [https://git.dhimmel.com/bitcoin-whitepaper/]
[2] Haber, Stuart, and W. Scott Stornetta. "How to time-stamp a digital document." *Conference on the Theory and Application of Cryptography*. Springer, Berlin, Heidelberg, 1990. [https://www.anf.es/pdf/Haber_Stornetta.pdf]
[3]Mazieres, David, and Dennis Shasha. "Building secure file systems out of Byzantine storage." *Proceedings of the twenty-first annual symposium on Principles of distributed computing*. 2002. [https://cs.nyu.edu/cs/faculty/shasha/papers/mazpodc.pdf]
[4]Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." *Concurrency: the Works of Leslie Lamport*. 2019. 203-226. [https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf]
[5]Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." *white paper* 3.37 (2014): 2-1.

[https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf]
[6]Hyperledger Fabric [https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html]
[7]Hyperledger Sawtooth [https://www.hyperledger.org/wp-content/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf]
[8]Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." *OsDI*. Vol. 99. No. 1999. 1999. [http://pmg.csail.mit.edu/papers/osdi99.pdf]
[9]Ongaro, Diego, and John Ousterhout. "In search of an understandable consensus algorithm (extended version)." (2013). [https://raft.github.io/raft.pdf]
[10]Proof of Elapsed Time - Intel [https://sawtooth.hyperledger.org/docs/core/releases/1.0/architecture/poet.html]
[11]King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." *self-published paper, August* 19.1 (2012). [https://www.peercoin.net/whitepapers/peercoin-paper.pdf]
[12]Jakobsson, Markus, and Ari Juels. "Proofs of Work and Bread Pudding Protocols (Extended Abstract). Secure Information Networks (s. 258-272)." (1999). [https://link.springer.com/content/pdf/10.1007/978-0-387-35568-9_18.pdf]
[13]NXT Whitepaper - NXT Community [https://nxtdocs.jelurida.com/Nxt_Whitepaper]
[14]Popov, Serguei. "The tangle." *White paper* 1.3 (2018). [https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf]
[15]Churyumov, Anton. "Byteball: A decentralized system for storage and transfer of value." *URL https://byteball. org/Byteball. pdf* (2016). [https://obyte.org/Byteball.pdf]
[16]Baird, Leemon, and Atul Luykx. "The Hashgraph protocol: Efficient asynchronous BFT for high-throughput distributed ledgers." *2020 International Conference on Omni-layer Intelligent Systems (COINS)*. IEEE, 2020. [https://www.hedera.com/hh-ieee_coins_paper-200516.pdf]
[17]Harris-Braun, Eric, Nicolas Luck, and Arthur Brock. "Holochain scalable agent-centric distributed computing DRAFT (ALPHA 1)-2/15/2018." (2018). [https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf]
[18]Radix DeFi Whitepaper [https://uploads-ssl.webflow.com/6053f7fca5bf627283b582c2/61d5a4583aad156a094c5628_Radix%20DeFi%20White%20Paper%20v2.05.pdf]
[19]Cäsar, Florian, et al. "A Parallelized BFT Consensus Protocol for Radix." (2020). [https://www.radixdlt.com/wp-content/uploads/2020/03/Cerberus-Whitepaper-v1.0.pdf]
[20]Hughes, Dan. "Radix-tempo." *Radix DTL Whitepaper* (2017).[https://daks2k3a4ib2z.cloudfront.net/59b6f7652473ae000158679b/59ca573e4873510001375b15_RadixDLT-Whitepaper-v1.1.pdf]