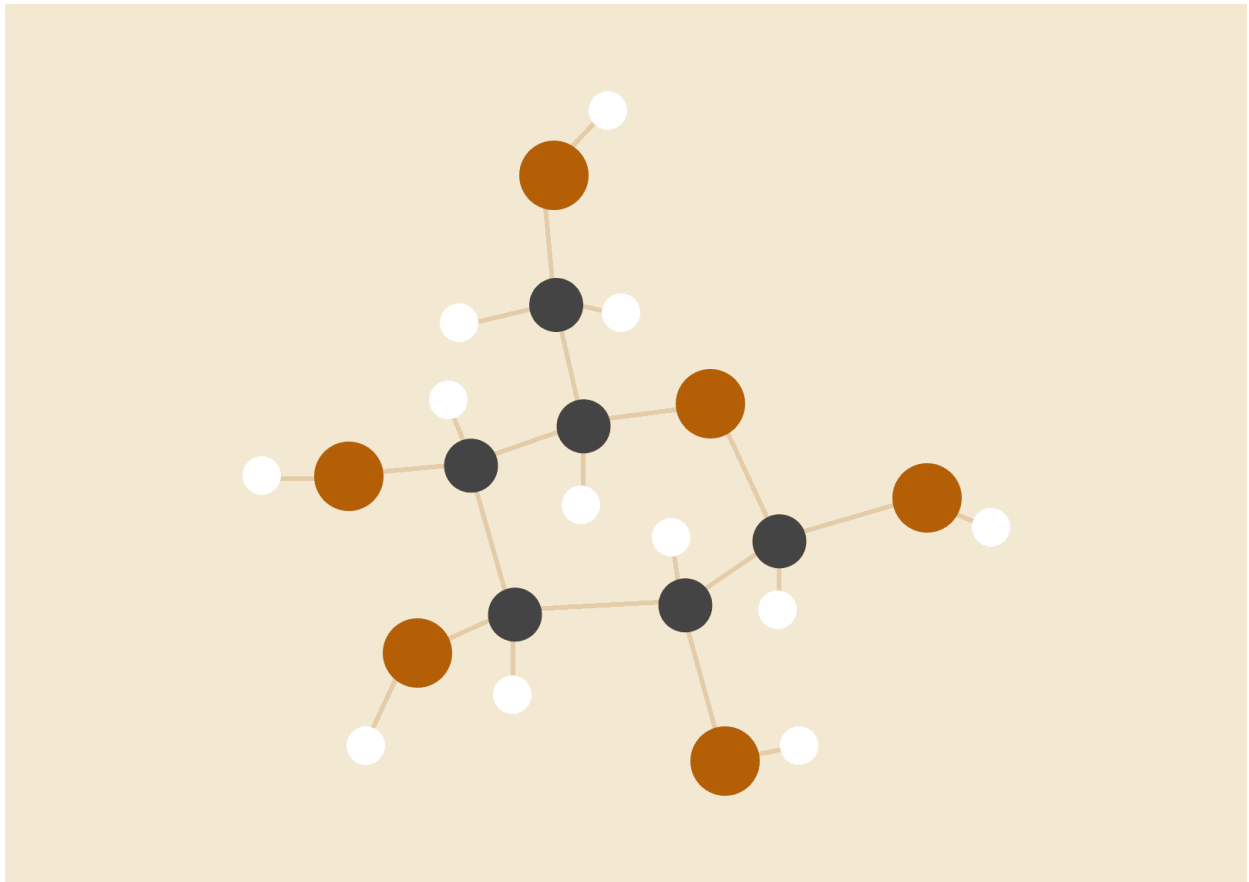


A Comparative Study into Blockchain and Alternative Distributed Ledger Technologies

Is Blockchain the only Solution?



Ali Raza (20i-2082) | **Usman Kaiser Moghal** (19i-1245)

Blockchain Project
13TH June 2021

INTRODUCTION

Given the sudden surge in cryptocurrency, a large number of influential bodies have shown an interest in blockchain and cryptocurrency. To deal in a cryptocurrency, we need to maintain a specialized relationship with other parties digitally, and the **need to have a secure digital relationship gives birth to the idea of blockchain**. Apart from cryptocurrency, any business would need to have a database for the purpose of keeping records of their transactions and maintaining logs. Above all, there would be a need for security. Standard databases do not fulfill this criteria.

In many businesses, having **multiple digital partners requires a middleman** to maintain fairness and sometimes middleman technology or central authority's function is expensive and time-consuming. There is a **need to have a secure and efficient option**.

Blockchain has the capability of providing a secure database with history. Secure distributed ledgers, immutable nature and no central point of attack makes blockchain unique from other databases and file systems.

However, is blockchain the only answer?

WHAT IS BLOCKCHAIN?

Blockchain in simpler terms is a computer file for storing digital information. It has the potential to provide secure distributed systems for any type of business. **Blockchain is technically a distributed database** which works as an efficient central authority between multiple digital partners. It has some data blocks connected with both its previous and next nodes, and that is how a chain of data blocks is built, hence the name blockchain.

These **data blocks are distributed** (i.e duplicated) over many computers which are part of the blockchain network. Each block of a blockchain contains not only information of its previous block but also holds the data about itself like when that block was created or edited, which makes it very useful for maintaining a detailed system of record that cannot be corrupted or lost.



Now because of the distributed nature of blockchain, the **security of data residing in the blocks is ensured**. Blockchain has a **decentralized record system**, so it doesn't need any administrator or administrative infrastructure that comes with other database and file systems. There is no single point entry for hackers in blockchain.

Types of Blockchain

There are mainly two types of blockchain, **Public** and **Private blockchains**, but due to some variations two more types **Consortium** and **Hybrid blockchains** exist. Before moving on towards these, let's just see some shared behaviors and rules between all these types of blockchain.

Every blockchain consists of clusters having nodes functioning on a **peer to peer system** throughout a network. Each and every node in a distributed ledger contains a copy of a shared information of blocks, so that each node in a cluster initiates, receives and verifies the legality of transactions.

Public Blockchain

Public blockchain is an **open source permission-less distributed ledger system**, which can be accessed easily throughout the internet. Anyone on the internet can sign up to this network and be a part of the blockchain network as a node. In this type of blockchain a user needs to follow the security rules strictly to avoid any risks. Users can perform cryptocurrency exchanges, mining and proof of work on this blockchain easily without any risks, if the security measures are followed strictly.

Examples: Ethereum, Bitcoin

Private Blockchain

Private blockchain is a **restrictive blockchain** functioning only in a **private closed network** which needs permission to enter and become a part of it. This type of

blockchain mostly operates within enterprises and organizations in which only limited members are part of the network and all the security measures like accessibility, authenticity, authorization and integrity are controlled by the organization itself. Thus private blockchain work similar to a public blockchain, except that it has a limited number of nodes.

Examples: Fabric, Sawtooth (Multichain projects) , Corda

Consortium Blockchain

Consortium blockchain is a **semi-decentralized distributed ledger**. It is more like a private network managed by more than one organization to exchange currencies and do mining. Each organization has some nodes which are part of this blockchain network, so it can also be referred to as a semi-private blockchain. This type of blockchain is usually used by different governments and banks for crypto sharing and mining.

Examples: R3,Energy Web Foundation etc.

Hybrid Blockchain

Hybrid blockchain **uses the functionality of both public and private blockchains**. In this type of blockchain users can have a public open source network as well as restrictive private systems. Users can have control on permissions on accessing the blocks in the network, only selected people have access to the transactions and records stored in private networks and some nodes are publicly accessible for verification. In hybrid mode all the transactions are verified within the private network but users can make it public for verification as the public blockchain has more secured verification nodes and steps, thus this adds transparency in this hybrid mode and makes it more secure.

LIMITATIONS OF BLOCKCHAIN

Blockchain is a great solution, however there are some issues in this technology. Some of the prominent ones are as follows:

Lack of Synergy

Blockchain is a distributed ledger and connects different organizations digitally, but it needs to be kept in mind that blockchain acts as a distributed storage system, and not a distributed computing system. Distributed computing systems don't depend on the **participation of every node** for computing and verification . Blockchain networks depend on nodes and their quality of assistance in terms of verification and functioning

properly, for example bitcoin gives incentives to the nodes to become a part of the network but not all blockchain give this facility to nodes in the network. Hence this adds up to its limitations in terms of mutual assistance and multi-tasking as compared to other distributed computing systems.

Energy Consumption

Blockchain technology was introduced with bitcoin in which we need some **consensus algorithm** as well as a need to do hard work as a miner to solve complex mathematical equations for **proof of work mechanism**. In the blockchain consensus algorithm we need to make sure that after every transaction each block in the blockchain must reach a common consensus. In blockchain, each block can be created in 10 minutes, meaning that this consensus mechanism consumes too many resources. Every time a ledger is updated in a network, miners need to solve problems which consume so much energy.

Drawbacks of Immutable Nature

Immutable behavior of blockchain really gives strength to the environment where we need to keep records of transactions and maintain its history. But not every financial supply chain wants this strict nature in their database and needs to do amendments on their records with the changing market requirements. Consider as an example, a bitcoin user who uses the blockchain and processes transactions, but now due to some unavoidable circumstances, the user needs to do **amendments in payments** but blockchain won't give you this liberty at any cost. Another example is that a user enters the blockchain network and becomes a part of it, now they want to leave this network and remove their trace from the network, but due to its limitation the users information is never removed from the network.

Scalability

Scalability is one of the biggest drawbacks of blockchain due its decentralized nature. Centralized systems typically don't have any scalability issues. Consider an example of the blockchain bitcoin, where every **bitcoin transaction** depends upon the network congestion in the blockchain. If more nodes join the network, it slows down in processing of transactions. There are some partial solutions to this scalability issue, in the form of private blockchains (having a limited number of nodes, so no congestion occurs), architectural blockchains (like Corda) and off blockchain transactions (in bitcoin). However none of these solutions have an ability to solve scalability issues in blockchain upto zero error.

Security Issues

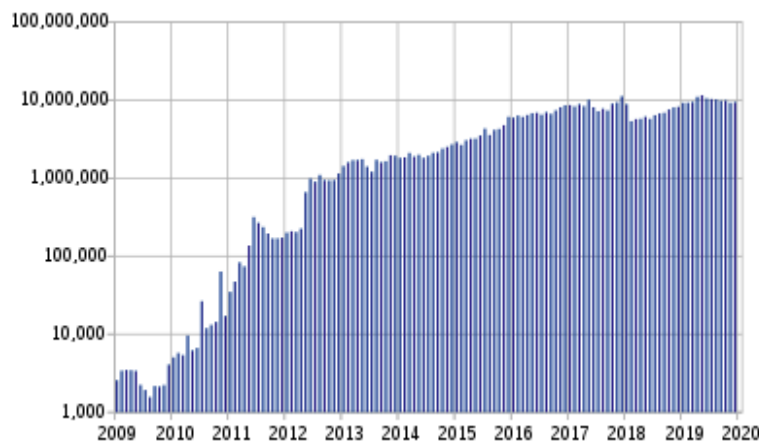
Blockchain is far more secure than other distributed or centralized platforms but still there are some vulnerabilities in blockchain technology which hackers could exploit. The following are some vulnerabilities in the blockchain network

- **51% Attack:** As blockchain operates on proof of work mechanism , if an entity controls 51% or more nodes, then they can easily modify and access ledger information which could compromise lots of integrity of users present in that network.
- **D-dos attack:** Nodes are bombarded with similar requests to a blockchain network and bring out congestion in the network which leads to compromise its accessibility.
- **Double Spending:** Proof of work mechanism solves double spending issue in blockchain but the networks vulnerable to 51% attack could still face this problem
- **Cryptographic cracking:** As we know blockchain works on cryptographic mechanism of keys and some quantum and computing algorithms nowadays are more than able to crack these cryptographic mechanisms.

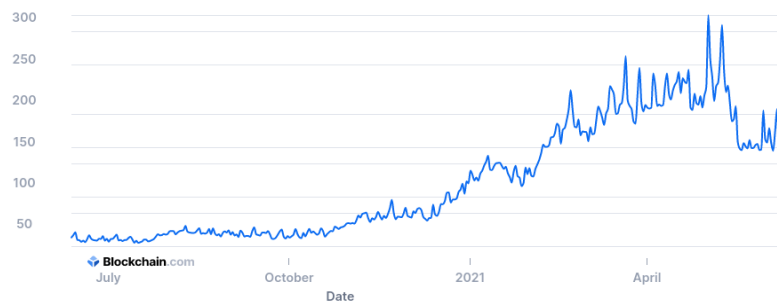
For more specific examples of how these issues surface within current applications, consider the following:

1- Bitcoin :

- If we see the graph of the number of transactions in bitcoin we can realize how big this scalability issue in blockchain is **[18]**.



- Transaction cost of blockchain also depends on its scalability and if we see the graph of transaction cost from July 2020 till now we can realize how much it affects miners [19].



2- Ethereum [20]

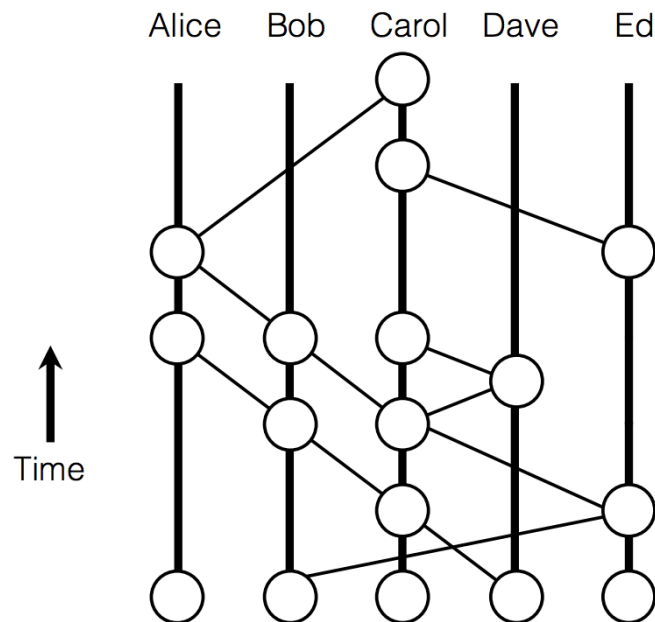
Given these shortcomings, alternate solutions need to be considered.

ALTERNATIVES TO BLOCKCHAIN

As bitcoin and other cryptocurrencies rose in popularity, a lot of research and development went into making blockchain, to make it better than what was originally proposed over 27 years ago. This push in **R&D gave birth to various other alternatives to blockchain**, with a few fundamental concepts in mind, namely scalability and higher transaction per second (TPS) capability.

There are many alternate distributed ledgers that are being used today for a variety of applications. Among them, some in particular stand out. They are as follows [1-7][12]:

Hashgraphs



Hashgraphs is a distributed ledger, which offers many of the benefits of blockchain, **without any limitation on the speed**, unlike in blockchain.

The main difference between Blockchain and Hashgraphs, is that **Hashgraphs use directed acyclic graphs** instead of blocks, which leads to a significant advantage to Hashgraphs by not being required to validate transactions.

Hashgraphs focus on consensus building, where transactions are dependent purely on consensus. This makes the network superior to blockchains through sheer robustness. **Purely relying on consensus** allows transactions to occur without the need for validations. Skipping this validation step increases TPS. Moreover, this eliminates the need for Proof of Work (PoW).

Consensus building can be done using techniques like “Gossip about Gossip” or “Virtual Voting Technique”.

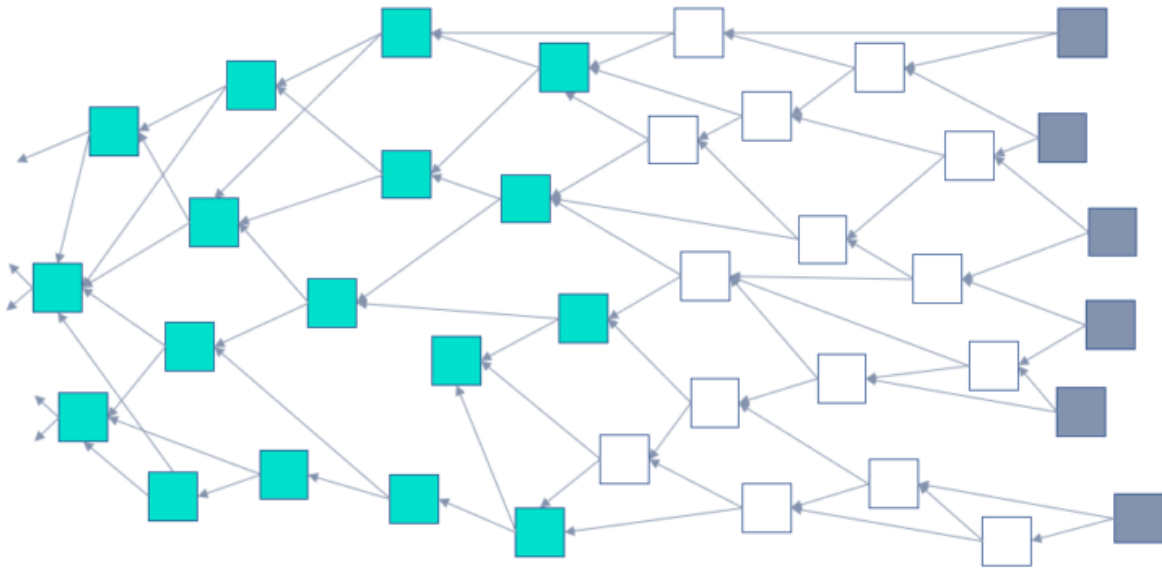
Hashgraphs also maintain fairness within their network, for instance, consensus timestamping avoids issues such as cancelling transactions as found in Blockchain.

This distributed ledger can even compete with some influential services like AWS, IBM, Oracle, Microsoft, etc.

Examples of Hashgraph include:

- Hedera

DAG



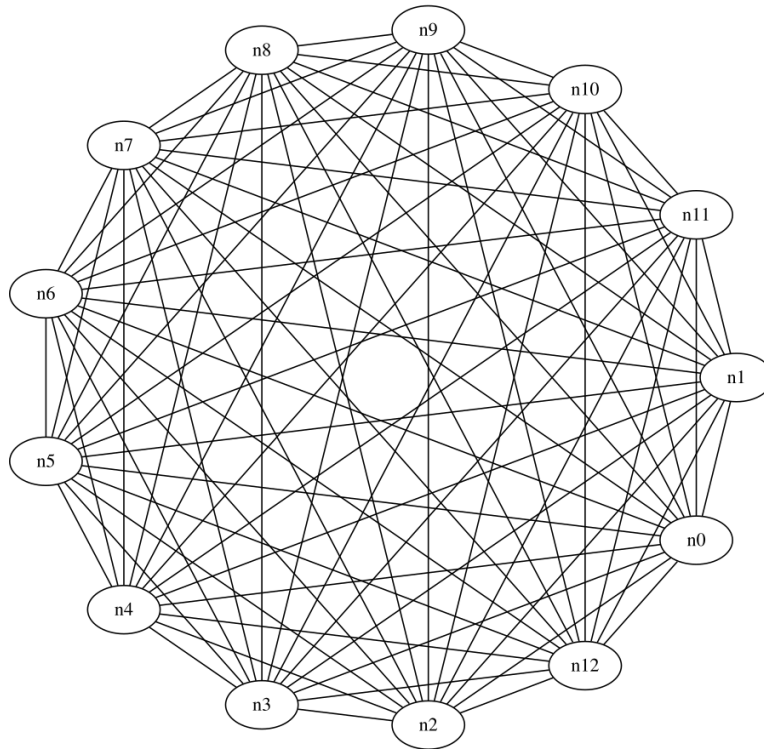
A **DAG is essentially a directed acyclic graph**, which is a typical data structure for storing information. One of the main benefits of a DAG is the **ability to topologically sort** a DAG. Various optimized algorithms exist for traversing through a DAG.

Similar to Hashgraphs, DAGs depend primarily on consensus within the network, specifically on majority support. Such a network has **greater cooperation between nodes**, with each node having equal rights.

Examples of DAG networks include:

- Byteball
- Tangle

Holochain



Developers claim that Holochain is the evolution of blockchain technology, and their goal is to change the current structure of the internet.

Holochain is a **DLT that prevents any centralization of flow of data**, by distributing power among its nodes. Each node will run on an independent chain, with the **users/miners autonomously operating**. This is possible using a distributed hash table (DHT), which is a data store utilizing certain keys, where the data is stored in physical locations across locations. Essentially, Holochain is a **combination of Blockchain, BitTorrent and Github**.

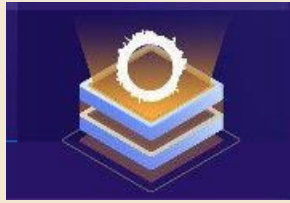
COMPARISONS BETWEEN BLOCKCHAIN AND ALTERNATIVES

Blockchain has various issues [17], such as limited scalability, large energy consumption, data immutability (depending on circumstances, it could be seen as positive or a negative), etc.

In lieu of these limitations, various developers have worked on different variants of DLTs.

In order to **optimize the efficiency of the DLT**, the major factor to be considered is the **type of task and the domain** the DLT will be used in.

Please see the table below for a generalized comparison between blockchain and some popular alternate DLTs [3-14][25-26]:

Features	 Blockchain	 Hashgraph	 DAG	 Holochain
Mining	Based on the consensus mechanism, new tokens can be minted	Consensus created through virtual voting	Consensus achieved through the validation of previous transactions	Transactions don't need to be validated, as nodes run on individual chains
Consensus	Proof of Work, Proof of Stake, etc.	VirtualVoting	Proof of Work, etc.	No consensus
Validation	Miners can postpone or cancel transactions	Based on consensus	The transactions preceding two transactions need to be validated	Nodes process their own ledgers
Technology	Block chain	Directed acyclic graph	Directed acyclic graph	Agent-centric
TPS	Limited	High	High	Limitless
Scalability	Limited	High	High	Limitless
Networks Currently in Use	BitCoin, Ethereum, etc.	Swirlds, NOIA, etc.	ByteBall, Tangle, etc.	Holochain
Major Drawback	Heavy resource consumption	Low communication frequency	Centralization concern	New, Slow validations

Unique Features	Smart contracts, Miners, Large number of implementations	Fairness, Virtual voting, Efficiency, High TPS	Scalability, Quantum computation, Micro-transactions	Scalability, High TPS, Security
Security	High	Very High	High	Very High
Best Used For	Trusted data verifications, monetary transactions, decentralized apps	Cryptocurrency, Time-sensitive Solutions, Smart Contracts, decentralized apps	Micro or nano transactions between devices or sensors	Issuance between peers, double-entry accounting, collective intelligence, collaboration
Privacy	Low	Low	Low	Low
Transaction Fee	Yes	No	No	No
Fairness	No	Yes	No	Yes
Node Competition	Yes	No	No	No

CONCLUSIONS

All DLTs provide various benefits, and can be used for almost any use case. However, to get the best result, it is critical to use the appropriate DLT for the given task.

An example of how important the given task is, and why a company would choose an alternate DLT, consider **Intivia Health**, who decided to use a Hashgraph instead of a Blockchain. They posted the following on their site [5]:

*“The Intiva Health Platform currently allows licensed medical professionals, facilities, and groups to streamline recruitment, expedite credentialing, and maintain compliance. Intiva Health will completely redefine the medical credentialing process by **integrating a Hashgraph-based, self-auditing solution** that will instantly verify provider’s credentials — **cutting months’ worth of processing time to a matter of seconds**. The Intiva Token (NTVA) builds on this idea and rewards users for time spent on our platform.”*

MOVING FORWARD

As popularity of DLTs increase, more and more research and development is being carried out on the respective DLTs. Various **vulnerabilities are being caught and fixed, with new improvements** being proposed.

With this rise in popularity, and alternatives to blockchain being more standardized, **researchers are beginning to look towards these DLTs for a myriad of new tasks.**

For instance:

- DLTs in Anti- Money laundering system
- Advertising insights using DLTs[23]
- DLTs in Real-time IoT operating systems [21]
- DLTs in Artificial Intelligence [21]
- DLTs in supply chain communication [22]

REFERENCES

1. <https://blog.eccouncil.org/blockchain-vs-hashgraph-vs-dag-vs-holochain-4-types-of-dlts/>
2. <https://blog.eccouncil.org/hashgraph-vs-blockchain-top-4-differences-you-need-to-know/>
3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144241
4. https://www.researchgate.net/publication/331687996_When_Internet_of_Things_Meets_Blockchain_Challenges_in_Distributed_Consensus
5. <https://medium.com/coinmonks/is-blockchain-alternative-hashgraph-really-a-game-changer-a-beginners-guide-a1bdadf959de>
6. <https://medium.com/@vardan.sevan/hashgraph-examples-of-consensus-protocols-6ca576cc1b8a>
7. <https://www.youtube.com/watch?v=JjMWrXqsrUs>
8. <https://101blockchains.com/hashgraph-vs-blockchain/>
9. <https://www.leewayhertz.com/hashgraph-vs-blockchain/>
10. <https://theblockchaindecentral.com/blockchain-vs-hashgraph-vs-dag-vs-holochain-types-of-dlts/>
11. <https://pupuweb.com/compare-dlt-blockchain-hashgraph-dag-holochain/>
12. <https://101blockchains.com/blockchain-vs-hashgraph-vs-dag-vs-holochain/>

13. <https://ieeexplore.ieee.org/abstract/document/8980029>
14. https://link.springer.com/chapter/10.1007/978-3-030-02671-4_16
15. <https://ieeexplore.ieee.org/abstract/document/8686563>
16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452709
17. <https://101blockchains.com/disadvantages-of-blockchain/>
18. https://en.wikipedia.org/wiki/Bitcoin_scalability_problem
19. <https://www.blockchain.com/charts/cost-per-transaction?>
20. <https://personal-financial.com/2020/10/05/benefits-and-limitations-of-ethereum-et-h/>
21. <https://www.ibm.com/blogs/blockchain/2020/08/how-blockchain-adds-trust-to-ai-and-iot/>
22. <https://link.springer.com/article/10.1007/s00530-020-00687-0>
23. <https://doi.org/10.1007/s00530-020-00687-0>
24. <https://www.searchenginewatch.com/2020/02/26/how-blockchain-will-dominate-the-digital-advertising-industry-in-2020/>
25. <https://maxthake.medium.com/what-is-dag-distributed-ledger-technology-8b182a858e19>
26. <https://holo.host/faq/what-is-holochain/>