Survey on the Performance Evaluation of Distributed Ledger Technology

Océane Pujol
Email : ocepu527@student.liu.se

Muhammad Nauman Afzal Khan Khan
Email : muhkh138@student.liu.se

Supervisor: Ioannis Avgouleas, ioannis.avgouleas@liu.se
Project Report for Information Security Course
Linköping University, Sweden

Abstract

Distributed ledger technology (DLT) is an evolutionary concept. Before that, financial services relayed on physical centralized data storage and trustworthy intermediaries' parties to perform transactions. The major change with DLTs is decentralization. It increases security and removes the intermediaries' parties.

In this report, we will first give a general overview of DLTs by presenting their characteristics and types as well as describing the inner workings of Blockchain technology. Then, we will go through the literature and present some of the most popular types of DLTs: Bitcoin, Ethereum, Hyperledger Fabric, and Multichain. Lastly, with all the information we gathered from existing papers, a comparison will be performed regarding the scalability and performance of each DLT presented.

The goal is to provide enough information regarding the performance and scalability of several DLTs so that one can choose the technology that is more appropriate for its use. Therefore, according to our results, Ethereum is more scalable, but Fabric and Multichain are more efficient.

1. Introduction

Technological advancement brings comfort and modernism to human life. Various traditional work methods have been completely changed. Back in time, records used to be kept in paper form. After the advent of computers, information was stored in databases. One thing is common in the ancient and modern way of keeping records, they both had centralized systems. Authorities keeping those records were the only source of record authentication. Such authorities (states, banks) often acted as trusted third parties. However, they had several points of failure and were vulnerable to information leakage.

The advent of bitcoin brings the revolutionary distributed ledger technology with solutions to the above-mentioned weaknesses in centralized systems. It is the new way of storing data and is particularly used for transactions. This technology brings out significant advantages over centralized systems. To understand DLT, one must understand the ledger. The record containing all debit and credit information of an account is known as a ledger. It is often used to develop financial statements. In distributed ledger technology, a ledger is stored in each node's database locally. All nodes are connected in a way that they create a decentralized peer-to-peer network. Therefore, the ledger is stored on each individual computer, not centrally in a server system. A distributed ledger can be either permissioned or permissionless. On one hand, a permissioned network only includes trusted members. They can access and modify the ledger. On the other hand, a permissionless network can be accessed and modified by anyone. The decentralized mechanism of DLT limits its performance. The performance is measured with the throughput and latency of the system. Throughput refers to the number of transactions processed within a given time. Latency indicates the time needed to complete a certain task. Each DLT is different and differs by its performance. Bitcoin, for example, can process up to 7 transactions/sec but it takes 10 minutes for a single transaction to get confirmed. In comparison, visa card (centralized payment system) confirms a transaction within seconds and process 2000 transaction/sec which is almost real-time payments [1]. Hence a significant difference exists between DLT and mainstream information systems.

In this paper, we first give a broad overview of the distributed ledger technology. Our goal is to give the reader a good understanding of what it is. Therefore, we briefly explain how a DLT works, its types, and its properties. We also explain how blockchain works as it is a broadly used technology. Secondly, with the existing literature, we describe four popular DLT platforms, which are the following: Bitcoin, Ethereum, Hyperledger Fabric, and Multichain. Thirdly, we do a comparison between the DLTs in terms of their performance and scalability. Finally, we present the results. The goal is to enable the reader to choose between several well-known DLTs regarding their needs.

Several surveys have been made to compare different DLTs applied to a specific field [2], [3]. Other studies have been made on their applications, investigating the effect on technology and business (see section 7. Related work). To our knowledge, no studies have been made regarding the comparison of some of the most popular DLTs which focused on both scalability and performance.

The remainder of this paper is structured as follows: The distributed ledger technology is first described, followed by a presentation of the chosen popular DLTs. Then, we compare those different platforms regarding scalability and performance. Finally, we present our conclusions.

2. Methodology

In this part, we will present the method used for this survey.

1) We search for papers in the literature using several databases, which are the LiU Library Catalog, Google Scholar, IEEExplore, and ScienceDirect. As soon as we gathered a few papers, we investigated their references to gather more papers.
2) To conduct our research, we searched for some specific keywords in the above databases. At first, we only searched for papers containing the expression "Distributed ledger". We quickly saw that the number of papers was limited. Thus, we used the following keywords together with the expression "Distributed ledger": "P2P network", "Performance", "Consensus algorithms", "Consensus mechanisms", "Bitcoin", "Multichain", "Ethereum" and "Hyperledger fabric", as those are our focus as stated in section 1.
3) After reading the title and abstract to ensure that the paper is related to our project, we only selected papers that are in English and considered recent, i.e published from 2016 to this date (March 2021).

We ended up having 56 papers from various databases, with the majority coming from IEEExplore and ScienceDirect. They were published in various years, with approximately 10 papers per year. We read them and kept only the papers that were the most relevant. We know our scale is not appropriate to study the change in popularity of this technology over time. Indeed, we would need a much larger collection of paper for such an evaluation. We note that according to Li et al. [2], papers about blockchain keep increasing as the years go by.

3. Short Overview of DLTs

The concept of distributed ledger technology was first presented in late 2008 with the concept of bitcoin, a blockchain-based technology, invented by a researcher with the pseudonym "Satoshi Nakamoto" [4]. It was first implemented in 2009. In the last decade, DLT gained extensive attention among various fields of life such as supply chain, financial services, healthcare [5], [6], finance, transport, education, governance, smart city, energy, manufacturing, and information technology [2]. It is considered a revolutionary concept that has changed the conventional working style of many applications.

Let us define this technology. A distributed ledger is a decentralized database whose ledger is distributed and stored by the nodes of a Peer-to-Peer (P2P) network [7]. Every participant (node) in the network is a client and server at the same time, sending and receiving data simultaneously. Distributed ledgers are append-only, none of their data can be removed [8].

The parties of a distributed ledger do not necessarily trust each other. To reach an agreement on what should be added to the ledger a set of rules and protocols must be followed by every participant. It is the consensus algorithm. Its primary role is to validate transactions and store data sequentially. It ensures that no duplicate or fraudulent information is in the ledger. It also verifies if all ledgers of the participants are identical [3], [9]. A wide range of consensus algorithms exists, the most popular one is the Proof-of-Work (PoW) which we will explain in detail later in this paper.

3.1. Properties

We will now present the main properties of a distributed ledger [7], [8], [3].

- Immutable, irreversible, and persistent: The fact that many participants store and confirm the ledger, consenting to the same rules makes it immutable and irreversible if the nodes are part of a P2P network. Moreover, as the ledger is an append-only data structure, the data persist over time.
- Transparent: Every single interaction can be verified by anyone with a copy of the ledger at any time, ensuring the transparency of the distributed ledger.
- Trust: In a distributed ledger, participants do not fully trust one another. The consensus algorithm makes sure that every node follows the rules, therefore bringing trust in the system.
- Single source of truth: Every transaction in a distributed ledger is signed with a public key cryptography mechanism. This algorithm ensures the authenticity of the data. When we know that DLTs are immutable and irreversible as well, this results in a piece of indisputable information applying for any data in the ledger.
- Anonymity: Asymmetric cryptography is used to make sure of the good integrity of the message as well as to authenticate the sender. Hence, cryptography performs an essential role in this scenario. Information is encrypted first, then sent from one node to another so that during the transaction no one manipulates the information. Each participant in the transaction has a private key and public key pair. The hash value of the public key is used as the participant's identity or transaction address. The private key is used to sign the transaction. The signature can later be verified by other parties using the signer's public key [10].
- Decentralized: One must have precise knowledge of the centralized and decentralized systems. In a centralized traditional distributed database, a central authority controls the whole network. The parties trust each other and cooperate to keep consistent data. Banks, for example, accept clients after a client verification process and have the power to cancel their membership without their permission. It means the service provider possesses all authority. But, in a decentralized system, things work differently. The participants do not trust each other completely, therefore a tool must be implemented to verify

ledgers cooperatively before they are shared. It is the consensus algorithm. A distributed ledger is decentralized as each transaction is stored multiple times over different participant's machines and confirmed according to a set of policies accepted by everyone in the ledger.

3.2. Types

There are two types of DLTs. A distributed ledger can be either permissioned or permissionless.

3.2.1. Permissionless DLT

They usually are public ledgers in which everyone can join and participate. This is the pioneer type of distributed ledger technology as Bitcoin is permissionless. Anyone can update, validate, and store the ledger. Each node (participant) can see any transaction that happened in the network. The ledger state and every transaction are therefore totally transparent. This can be a concern regarding privacy if the data should be preserved [7]. As there is no client authentication process, the network remains anonymous. To encourage people to do transactions and validate them, an incentive system is required. Users are rewarded when they participate in network activities. Moreover, cryptography and other security measures make public DLTs more secure as they can have many participating nodes.

However, permissionless DLTs are not energy efficient. Indeed, most of the Public DLTs require a large amount of computational power to validate a single transaction because they are required to solve complex cryptographic problems. Therefore, they are not very efficient (low transaction per second). Our paper will examine these weaknesses more carefully and dig deeper into two well-known Public distributed Ledger: Ethereum and Bitcoin.

3.2.2. Permissioned DLT

Permissioned distributed ledgers are usually used in private DLTs as their access is regulated. Private organizations, e.g., companies, institutes, industries, and banks, that want to secure their information and need fair regulation often adopt permissioned ledger. The permissioned network becomes private when every contribution and access is verified. The purpose of a private shared ledger is to avoid it from being public. The permissioned ledger is restricted as only authorized and trusted parties can join it [11]. Consequently, a private DLT ensures the privacy of the ledger, which might be put to good use in some cases. The entities must be authorized or invited by a "centralized trusted identity management system" [3] to join the network. The nodes are assigned different privileges regarding their identities.

Compared to public ledgers, private DLTs are more efficient. As there are way fewer nodes in a private ledger, it consumes less energy for validating new information. However, the security risk rises in those ledgers as not many people can validate a transaction compared to public DLTs [12]. Private shared ledgers are fast, scalable, and energy-efficient. Organizations can customize networks according to their requirements. They are often used for research, financial institutions projects, internal voting, and supply chain management. There are multiple permissioned DLTs, but we will only discuss Hyperledger fabric and Multichain in this paper.

3.3. Blockchain architecture

Blockchain was first invented to support cryptocurrencies. It is often used as a generic term for distributed ledger technology. However, it is a specific type of decentralized shared ledger that uses chronological, encrypted, and chained blocks to store verifiable and synchronized data across a Peer-to-Peer network.

Blockchain architecture can be easily understood by explaining each of its layers. Li et al. [2], Yuan et al. [13] and Xu et al. [14] presented a 6 layers architecture, whereas Fan et al. [15] described a 5 layers blockchain model and Yuan et al. [16] came up with a 7 layers architecture for ITS (Intelligent Transportation System), a use-case in IoT domain.

We here choose to detail the 6 layers architecture of blockchain as it seems to be the most common one. Figure 1 is a scheme of the different layers in blockchain architecture.

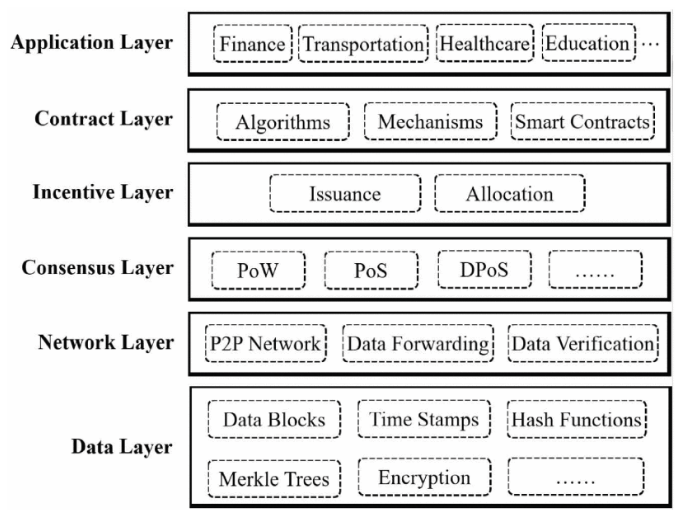

Fig. 1. Reference model of blockchain [13].

3.3.1. Data Layer

In the data layer, the data is encapsulated in chained blocks, stored on the nodes of the blockchain network. The blocks contain asymmetric encryption (public and private keys), hash values, time stamps, Merkle trees, and transaction information that connects it to the prior block [3]. The timestamp indicates the creation time of a block.

As shown in Figure 2 below, a block is composed of a header, which contains all meta-information, and a body enclosing a Merkle tree of the verified and hash data [17]. A Merkle tree or hash tree is a data structure containing a summary of information from a volume of data, usually large.

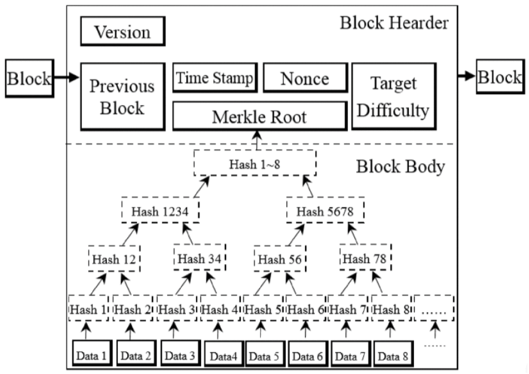

Fig. 2. Structure of a block in blockchain [16].

3.3.2. Network Layer

The network layer specifies the decentralized networking mechanisms, data broadcasting, and verification. Blockchain is based on a peer-to-peer network. In its many applications, blockchain involves many nodes. All the nodes are equal, without any centralized entity. The resources in the blockchain network are shared and verified by every node. The network layer is where nodes synchronize information.

3.3.3. Consensus Layer

In the consensus layer, the consensus algorithm is encapsulated. It enables the nodes to reach a consensus on the validity of the blocks. Therefore, consistency is kept among the nodes. This algorithm also decides which block will be submitted next [18].

3.3.4. Incentive Layer

In public ledgers, the incentive layer is here to encourage people with economic rewards to participate in the activities and follow the rules. In private ledgers, the incentive mechanism does not exist because they are less decentralized. Indeed, the participants must take part in the activities in the ledger.

3.3.5. Contract Layer

In the contract layer, various mechanisms, code, algorithms, and smart contracts are encapsulated. They serve as a base for the programmability of the blockchain. Smart contracts are a set of rules that verify, execute, and enforce themselves. When several parties in a blockchain network agree to a set of rules, they write them in a smart contract to be verified and stored in a block. Once a precondition appears, the associated actions will be executed without third parties as shown in figure 3 below.

With smart contracts, decentralized applications (DApps) and decentralized autonomous organizations (DAOs) can be created [19]. A DAO is an autonomous program that does not need to rely on a system operator to work, it only follows the rules written in the smart contract. A DApp includes a decentralized backend and a front-end user interface to interact with Blockchain and smart contracts.

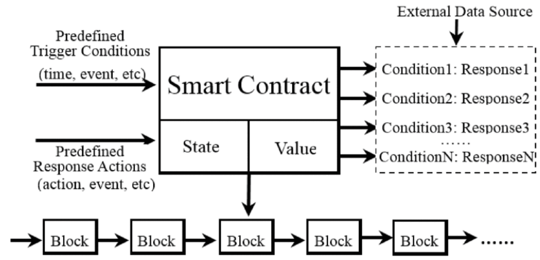

Fig. 3. Smart contract in blockchain [13]

3.3.6. Application Layer

In the application layer, all sorts of application scenarios and use-cases of blockchain are encapsulated. For example, Mengelkamp et al.'s work [20] presents a blockchain-based solution for the local power generation market. Also, Yuan et al. [16], studied an intelligent transport system created from the architecture of the blockchain. Finally, Kosba et al. [21] shows a new smart contract, "Hawk", allowing not to broadcast financial transactions in the clear. More and more applications for blockchain are invented every year. With the power of smart contracts and the solid foundations of blockchain technology, the possibilities are broad and have potential implications in all sectors of technology and society.

4. Different DLTs platforms

We will now present each DLT platform that will be compared in the next section of this report. We choose to study Bitcoin, Ethereum, Hyperledger Fabric, and Multichain because they are some of the most used and popular.

4.1. Bitcoin

Bitcoin is the decentralized cryptocurrency that introduced blockchain, as well as DLTs [4]. It might have been created because of the global economic crisis in 2008 to offer an alternative to the central-bank system [3]. It is a public permissionless ledger, meaning that everyone can join, update, and interact with the Bitcoin network. This blockchain-based cryptocurrency is mainly used for payment by transactions of bitcoin from one entity to another. Bitcoin is a large-scale technology that was adopted worldwide.

It uses crypto assets as remuneration for validation as part of the incentive mechanism [8]. If the same bitcoin address is used for several transactions, there could be a privacy issue. Therefore, participants are encouraged to generate a new address for each transaction. As it is hard to manage, an application called wallet is used to store and generate public and private key pairs [22].

A lot of cryptocurrencies have been created since bitcoin's appearance. They are usually invented to avoid some security or privacy flaws of Bitcoin or to adapt it to different business use-cases. Even with those new crypto-currencies, bitcoin remains the most important blockchain application today.

4.1.1. Proof-of-Work

The proof-of-work (PoW) is the consensus algorithm used by Bitcoin and is the most adopted one. It is also the consensus algorithm used in Ethereum, another Blockchain technology that we will study later.

Also called Nakamoto consensus or mining process, it is designed to solve a complex computational crypto puzzle which required to generate a cryptographic hash with specific properties. This hard puzzle must be solved for each validation and creation of a new block [23], [24]. It is a competitive process as the first miner to solve the puzzle gets the bitcoin reward and the right to broadcast the new block on the bitcoin network. Other parties only accept the block if the transaction is valid and not already spent, therefore, avoiding double-spent fraud [25].

According to Cao et al. [26] and the original paper describing Bitcoin [4] the puzzle is the following : find a nonce N to add to the previous block B, that when hashed together will be equal or lower to a very small number defined as the inverse of the target difficulty D. We are looking for a N such that :

$$B + N \mapsto U \leq \frac{1}{D} \leq 1$$

U is the hash value, used as the "previous hash" to add to the next block, as seen in figure 4. The difficulty D is continuously adjusted by moving average so that a new block is mined approximately every 10 minutes. All other nodes can easily check the correctness of the solution with a single hash operation.

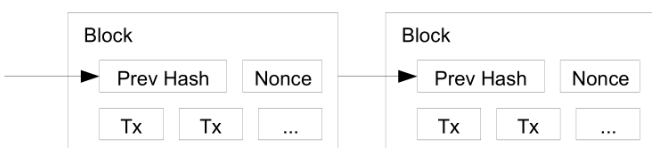

Fig. 4. Linked chain of blocks [4]

Because every new block contains the hash value of the previous, they are all linked by a chain of hashes. Submitting a new branch of the blockchain altering the previously made transactions would require computing an entire series of new hashes, a computing problem requiring resources deemed too high in real-time.

This consensus algorithm ensures the validity and the order of the block created among all participants, allowing the data storage to be accurate. The ledger mainly consists of a series of transactions outlining how Bitcoin currency circulates among the participants. For more theory on the proof-of-work consensus algorithm, read the work of Cao et al. [26].

4.2. Ethereum

In 2017, Ethereum was the second largest permissionless network, it was first presented in 2015 [24]. It is meant to execute smart contracts, which is done in a virtual machine, called Ethereum virtual machine (EVM). The state of the EVM, as well as the added ledger data, are stored in the distributed ledger. Like Bitcoin, Ethereum provides a payment system with the currency Ether.

Code execution requires storage on accounts, two types exist: Contract Account (CA) and Externally Owned Account (EOA). An EOA manages its balance. A CA has its code and storage and executes it when a message is received. The code is written with the language Solidity [22], [27].

Executing smart contracts costs "gas" fees that are paid with Ether, Ethereum's cryptocurrency. This fee is a way to avoid the computer from being abused and therefore avoid the infinite loops. Indeed, if the node is out of "gas" the code execution will stop. Ethereum is currently using PoW as a consensus algorithm. It is planned to upgrade to the Proof-of-Stake (PoS) consensus algorithm [28].

4.2.1. Proof-of-Stake

Proof-of-Stake (PoS) is an evolution from PoW, adding fairness between miners, decreasing computing power competition in the consensus algorithm [26]. The crypto-puzzle is the same as in the Proof-of-Work, only the target difficulty is weighted for each miner i depending on their stake in the blockchain (bal_i amount of currency owned by the miner) and their mining results (time since last winning t_i). Therefore, the computing condition to satisfy is the following one :

$$U \leq \frac{bal_i \times t_i}{D} \leq 1$$

Thus, the higher the balance, the lower the difficulty, making the puzzle easier to solve. Similarly, the later the date of the last winning, the lower the difficulty, making solving the puzzle easier. This results in fairness when it comes to the winner. Having a high balance and a long time from the last win gives an advantage and balances users' chances of winning the validation. The winner known as the validator must do the validation. If he does not, the next winner is chosen. This fairness improvement should stop the need for currently enormous and growing amounts of computation power and energy required to mine PoW cryptocurrencies.

4.3. Hyperledger Fabric

Hyperledger is an open-source project created by the Linux Foundation in 2016 to improve the performance and reliability of blockchain technologies. It is composed of 5 Hyperledger frameworks: Burrow, Fabric, Indy, Iroha, and Sawtooth. We will only study the Hyperledger Fabric framework as it is the most popular one, but first, let us see how the generalized Hyperledger consensus process flow.

4.3.1. Generalized view of consensus in Hyperledger

The process shown in figure 5 is the common way to achieve consensus in the Hyperledger frameworks. However, the different frameworks might implement some steps of this process differently. Usually, there are two steps to achieve consensus :

1) Ordering of transactions
2) Validating transactions

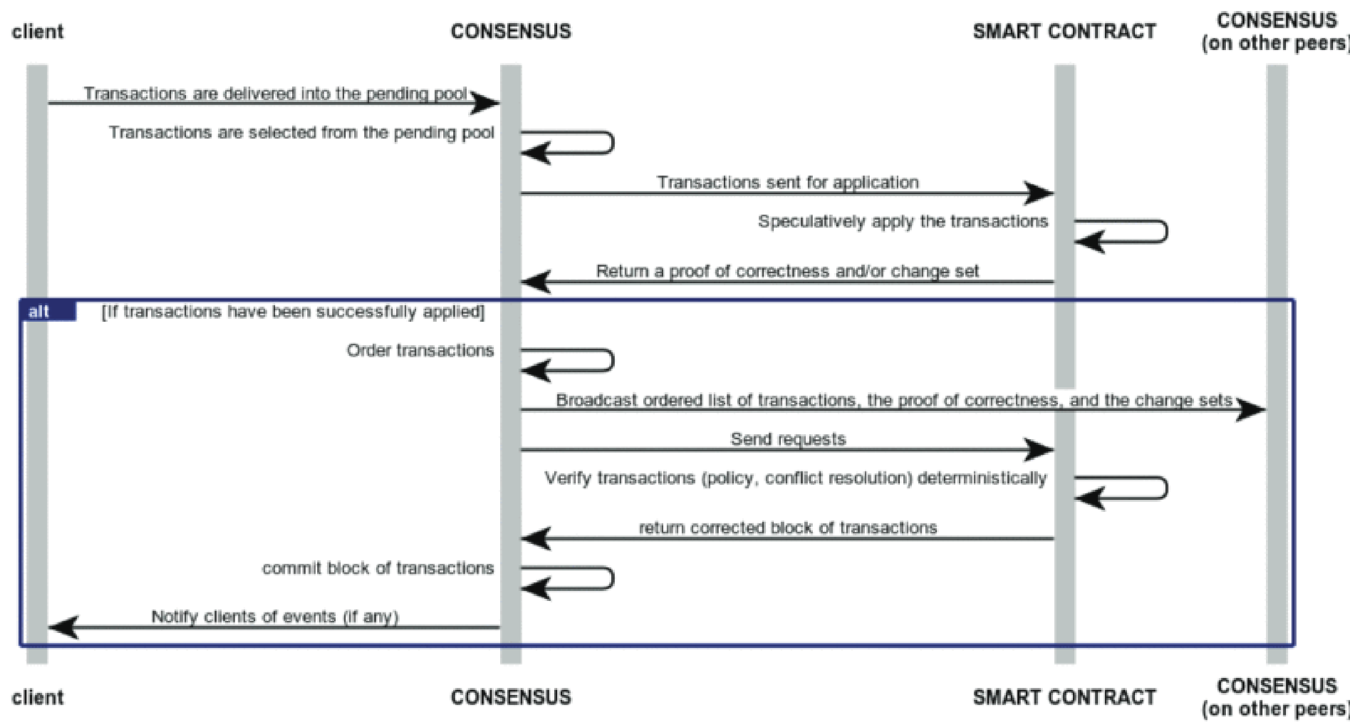

Fig. 5. Generalized Hyperledger consensus process flow [7]

First, the transactions from the client application are received.

Then, they are submitted to the ordering service responsible for ordering transactions. Consensus depends on it. There are different ways to implement the ordering service, from a centralized service to distributed protocols. Also, the content of the transactions can be encrypted or hashed to enable confidentiality. This service collects transactions based on the consensus algorithm and configuration policy, which may define a time limit or specify the number of transactions allowed.

Next, the transactions are validated by the smart contract layer. It ensures that they conform to the policy and the contract specified. The invalid transactions are rejected.

Finally, the consensus layer uses the communication layer for communicating with the client and other peers on the network to order, broadcast, verify and commit the validated transactions.

4.3.2. Hyperledger Fabric consensus process

Hyperledger Fabric is a platform allowing the user to create a permissioned and private blockchain hosted by the Linux Foundation. To ensure that this blockchain corresponds to business and organizations' use-cases, it has been created in a way that strong privacy is implemented. Each node in the ledger must be identified and therefore needs to be registered in the Membership Service Provider (MSP). With this identity, it is possible to create security policies. To improve privacy, even more, it is possible to create channels with a group of members who will have access to a separate ledger [28].

Fabric has a rare feature in DLTs: it can maintain several ledgers at a time. Also, the main advantage of the Hyperledger Fabric framework is its modularity. For example, it can support several consensus algorithms (SOLO, Kafka, and soon Simplified Byzantine Fault Tolerance-SBFT) as well as several algorithms for identification and encryption.

In Fabric, a smart contract is known as a chaincode. It can currently be written in Go and Java. It is a computer program that is deployed on the ledger and can interact with the data in the ledger. A chaincode has an endorsement policy that specifies the number and the identity of the peers who must verify and endorse a transaction [29]. An important concept in Fabric is the orderer entity. It is the node that creates a block and adds it in the correct order in the ledger. Other entities are the endorsers. They validate a transaction and check if the transaction follows the endorsement policy, resulting in the validation or invalidation of the block [30], [31].

A transaction flow in Fabric is divided into three phases [32], illustrated in figure 6. In the execute phase, the client sends a transaction proposal to all the endorsing peers (step 1). If the transaction is appropriate, they return the endorsed transaction to the client (step 2). In the ordering phase, the client sends the transaction and the endorsement to the orderer entity (step 3) The orderer adds the block in the correct order in the blockchain. In the validation phase, the block is returned to all peers in the ledger (step 4). They all append the new block to their local blockchain and validate the transactions in the block. If all checks are passed the client is notified of the successful transaction (step 5). If a step fails, the block is marked as invalid.

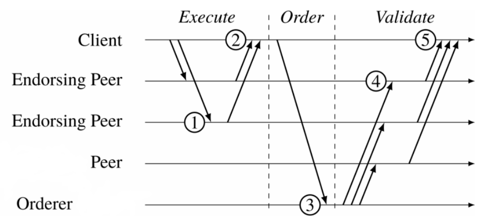

Fig. 6. Hyperledger fabric message flow [29]

We will now quickly describe the consensus mechanisms supported or to be supported by the Hyperledger Fabric framework.

4.3.3. SOLO

SOLO consists of just one single ordering node and thus, cannot provide any type of fault tolerance. It is a Hyperledger Fabric ordering mechanism most typically used only to test the Blockchain created. It is not used in a production environment.

4.3.4. Kafka

Kafka is an ordering service implementation in which only the leader does the ordering. This implementation for nodes configuration is called "leader and follower" and is managed using Zookeeper Ensembled, a distributed coordination service. This provides crash fault-tolerance which is a mechanism in which the process will continue even when some of the existing nodes experience some failures while other nodes can still run.

4.3.5. Simplified Byzantine Fault Tolerance

In the Simplified Byzantine Fault Tolerance algorithm, the block's validator is a known entity. New blocks of transactions are created and proposed by this entity. To reach consensus, at least 2N+1 node must accept the block, where N is the number of malicious or non-functioning nodes. The Hyperledger Fabric framework was not originally designed to support Byzantine Fault Tolerance.

4.4. Multichain

Multichain is an open-source platform that enables the creation of permissioned blockchain deployed within or between organizations. Multichain is derived from the Bitcoin core software and provides a simple application interface (API) as well as a command-line interface (CLI) [33]. It allows the user to configure many parameters such as permitted transaction, maximum block size, mining reward, etc...

Multichain solves the main problems of bitcoin which are openness, mining, and privacy. First, with Multichain, you can ensure that only the chosen nodes can see the blockchain activity. Then, it is possible to control the transactions. Finally, Multichain avoids the proof-of-work costs in energy and computational power.

In the ledger, participants identify each other with a public address which is related to a private key. Each party randomly generates its private key. The public address is used for receiving funds and one can send those funds only by signing the transaction with the private key associated [3]. Multichain also enables the verification of the other participants' identities. Before a transaction, a "handshaking" process occurs between the nodes.

1) The two participants present their public addresses on the permitted lists.
2) Each party has a version of the permitted list and verifies if the other participant is on it.
3) The two nodes send a challenge message to each other.
4) Each party signs the challenge message with their private key associated with the public address they presented, proving their identity.

If any of the nodes disagree in any of the steps mentioned above, the peer-to-peer connection is aborted [7].

A distributed consensus among identified validators is used in Multichain, ensuring that mining is possible only for a set of identifiable parties. To establish a fair mining policy, in Multichain, the blocks must be created by permitted miners in rotation, otherwise, the blockchain is invalid. Also, a limit can be defined for the number of blocks that a miner can generate within a given interval of time. The reward for creating a new block in Multichain is set to zero by default but it can be modified. The Multichain 2.0 released in 2018, supports smart contracts.

5. Comparison of the DLTs

Let us now compare the different platforms described in section 4. The DLTs are generally compared regarding the following evaluation metrics: Scalability, Performance, Cost, Security, Privacy, Suitability, Resource Consumption, Robustness, and Resilience (non-exhaustive list). To reduce the scope of our study, we will concentrate our comparison only on Scalability and Performance.

Scalability refers to the ability of a particular technology to adapt to an order of magnitude change, in particular its ability to maintain functionality and performance. The more the system is scalable, the more it can be easily used in different scenarios. Performance is defined by the amount of data that a system can process within a period. Those three following parameters determine the scalability and performance of a system [25]:

- Block size: It specifies the maximum allowed size of a block in a distributed ledger. With a higher block size, more data can be processed by a given DLT. It enables the measurement of the scalability of the distributed technology.
- Block creation time: It indicates the average block creation time of a DLT. It depends on the consensus algorithm used by the ledger [35]. It is used to evaluate the performance and scalability of the DLT.
- Throughput: measured in transaction per second (TPS), it is the rate at which the transaction is added to the ledger [30]. It is used to measure the performance of a system.

DLT Plateform	Type	Consensus algorithm	Currency	Scalability and Performance			Energy
				Block Size	Block Time	Throughput (TPS)	
Bitcoin	Permssionless	PoW	Bitcoin	1MB	10 min	4 avg., 7 theoretical maximum	High
Ethereum	Permissionless	Pow	Ether	Implicit restriction ("gas" limit)	12 sec	No max ("gas" limit)	High
Fabric	Permissioned	Orderers and endorsers	None	Configurable	0,5-2sec	> 10k	Very low
Multichain	Permissioned	Distributed consensus among identified validators	None	Configurable (up to 1GB)	Configurable (down to 2 sec)	> 1k	Verylow

Fig. 7. Comparison of the considered distributed ledger [2], [7], [33], [34]

The energy column indicates the electrical energy consumption needed for running a consensus algorithm to create a new block. The consensus algorithm used greatly impacts the block creation time and the energy consumption of a DLT. The comparison of the DLT platforms is shown in figure 7.

In Hyperledger Fabric and Multichain, blocks are created over a short time and they have a high throughput. Hence, those two are best for the performance and as the block size is configurable, they are rather scalable. The advantage of multichain compared to Fabric is the number of parameters configurable by the user, whereas Fabric seems to be more performant.

The block size is limited for every platform we considered except for Ethereum for which the only limitation is the ”gas” limit. Even if the block creation time is not the fastest of all the DLTs compared, it is rather quick. Those two parameters enable the good scalability of Ethereum. Plus, the throughput is also theoretically unlimited. Thus, Ethereum is the best for scalability and is rather performant.

Among the four DLT platforms studied, Bitcoin is the worst in terms of scalability and performance as the Block size is fix and small compared to the other three, the block creation time is very long, and the throughput is slow.

As Bitcoin and Ethereum use the PoW, they consume more energy and need more computational power. This problem has led to the search for other more efficient consensus mechanisms (e.g., PoS) [8].

6. Discussion

In this section, we will be discussing the points that are worth noticing regarding the papers we gathered.

First, while reading the papers, we found an unclear concept. Some papers described several types of DLTs in a data structure way. Panwar et al. [36] mentioned 5 types of DLTs (Blockchain, Hashgraph, Holochain, DAG-Directed Acyclic Graph, and Tempo), Fan et al. [15] described 3 types of DLTs (Blockchain, DAG, and others). Most of the other papers studied did not mention these types at all. Some stated that DAG was a Blockchain ledger with a different consensus algorithm [26].

Then, we noticed that several papers that we gathered would not discuss existing blockchain technologies but come up with new ones adapted to some specific use-cases or domains. For example, Niya et al. [37] propose a new blockchain-based technology for IoT (Internet of Things). Kokoris-Kogias et al. [38], came up with a new blockchain that competes with the Visa performances. This is an illustration of the popularity of blockchain.

7. Related work

Chowdhury et al. [7] performed, in 2019, a comparison between several distributed ledger technology platforms. The paper describes the main characteristics of the technology and explains how the following platforms work: Bitcoin, Ethereum, Multichain, EOS, Cardano, Hyperledger Fabric, Hyperledger Sawtooth, Hyperledger Burrow, IOTA, Corda, and Waltonchain. Then, they compared quantitatively and qualitatively all the platforms. However, they do not provide a comparison of the performance of the different platforms.

In 2021, Li et al. [2] published a survey on Blockchain applied to the industry. They first explain how they gathered the papers from the literature and classify them. Then, a small overview of DLTs is given. Finally, they presented several blockchain use-cases in the industry domain.

Shen et al. [3], in 2018, performed a literature review of blockchain in cities. First, an explanation of DLTs was provided. Then, the methodology to gather and classify the paper was explained. Finally, they presented several blockchain-based use cases for cities.

8. Results and Conclusion

Distributed ledger technology is broad and complex. Understanding the key differences between the many ways it can be implemented is required to select the one fitting a user's need. Choosing the wrong platform will cause difficulties and some fixed limitations in the performance and scalability of the application relying on a DLT.

As a result of or survey, we would give the following advice:

1) If one needs a more scalable DLT, one should use Ethereum
2) For better performance, the user should use one of the permissioned ledgers studied. Multichain is more configurable, and Hyperledger Fabric is a bit more performant.

Bitcoin, Ethereum, and public ledgers, in general, are generating a lot of pollution, mainly because of their growing computation requirement for profitable mining. However, version 2.0 of Ethereum relying on a new fair consensus algorithm is currently being created to require less energy to operate [39]. In the future, we expect to see this technology continue to grow and evolve, as seen with more and more blockchain-based technologies invented every year. Also, in this survey, we set aside all other aspects of the different DLTs platforms. For example, the fact that public DLTs are more secure thanks to their number of nodes. Considering every single aspect of those four DLT platforms would be for further research and another survey.

References

[1] K. Croman, C.Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, , and R. Wattenhofer, "On scaling decentralized blockchains," *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, pp. 106–125, 2016.

[2] Z. Li, R. Y. Zhong, Z. Tian, H.-N. Dai, A. V. Barenji, and G. Q. Huang, "Industrial blockchain: A state-of-the-art survey," *Robotics and Computer-Integrated Manufacturing*, vol. 70, pp. 102–124, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0736584521000107

[3] C. Shen and F. Pena-Mora, "Blockchain for cities—a systematic literature review," *IEEE Access*, vol. 6, pp. 76 787–76 819, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8531608

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[5] T.-T. Kuo, H. Zavaleta Rojas, and L. Ohno-Machado, "Comparison of blockchain platforms: a systematic review and healthcare examples," *Journal of the American Medical Informatics Association*, vol. 26, no. 5, pp. 462–478, 03 2019. [Online]. Available: https://doi.org/10.1093/jamia/ocy185

[6] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "How blockchain could empower ehealth: An application for radiation oncology," in *Data Management and Analytics for Medicine and Healthcare*, E. Begoli, F. Wang, and G. Luo, Eds. Cham: Springer International Publishing, 2017, pp. 3–6.

[7] M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury, A. S. M. Kayes, M. Alazab, and P. Watters, "A comparative analysis of distributed ledger technology platforms," *IEEE Access*, vol. 7, pp. 167 930–167 943, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8902067

[8] J. L. R. Ugarte, "Distributed ledger technology (dlt): introduction," *Economic Bulletin*, no. DEC, pp. 1–11, 2018. [Online]. Available: https://ideas.repec.org/a/bde/journl/y2018i12daan26.html

[9] A. Collomb and K. Sok, "Blockchain / distributed ledger technology (dlt): What impact on the financial sector?" 2016.

[10] B. Fu, Z. Shu, and X. Liu, "Blockchain enhanced emission trading framework in fashion apparel manufacturing industry," *Sustainability (Switzerland)*, vol. 10, no. 4, 2018.

[11] Y. Bakos, H. Halaburda, and C. Mueller-Bloch, "When permissioned blockchains deliver more decentralization than permissionless," 2021.

[12] A. B. Haque and M. Rahman, "Blockchain technology: Methodology, application and security issues," 2020.

[13] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8419306

[14] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," in *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, 2017, pp. 128–133. [Online]. Available: https://ieeexplore.ieee.org/document/7940229

[15] C. Fan, S. Ghaemi, H. Khazaei, and P. Musilek, "Performance evaluation of blockchain systems: A systematic survey," *IEEE Access*, vol. 8, pp. 126 927–126 950, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9129732

[16] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, 2016, pp. 2663–2668. [Online]. Available: https://ieeexplore.ieee.org/document/7795984

[17] K. Leng, Y. Bi, L. Jing, H.-C. Fu, and I. Van Nieuwenhuyse, "Research on agricultural supply chain system with double chain architecture based on blockchain technology," *Future Generation Computer Systems*, vol. 86, pp. 641–649, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18304527

[18] R. Srivastava, S. Kumar, A. Singh, and H. M. Saraswat, "Blockchain : A revolutionary technology," *International Journal of Trend in Scientific Research and Development (ijtsrd)*, vol. 2, pp. 2368–2373, 2018. [Online]. Available: https://www.ijtsrd.com/papers/ijtsrd12751.pdf

[19] F. Victor, P. Ruppel, and A. Kupper, "A taxonomy for distributed ledger analytics," *Computer*, vol. 54, no. 2, pp. 30–38, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9353516

[20] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science - Research and Development*, vol. 33, pp. 207–214, 2018. [Online]. Available: https://link-springer-com.e.bibl.liu.se/article/10.1007/s00450-017-0360-9

[21] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 839–858.

[22] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17 465–17 477, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7961146

[23] J. F. Hoops, "An introduction to public and private distributed ledgers," 2017.

[24] S. Meunier, "Blockchain 101: What is blockchain and how does this revolutionary technology work?" in *Transforming Climate Finance and Green Investment with Blockchains*, 2018, pp. 23–34. [Online]. Available: https://www.proquest.com/docview/2136146834

[25] M. Macdonald, L. Liu-Thorrold, and R. Julien, "The blockchain: A comparison of platforms and their uses beyond bitcoin," 02 2017.

[26] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of pow, pos and dag based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864819301476

[27] S. Rouhani and R. Deters, "Performance analysis of ethereum transactions in private blockchain," in *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2017, pp. 70–74. [Online]. Available: https://ieeexplore.ieee.org/document/8342866

[28] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," in *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, 2018, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/8376323

[29] F. Geyer, H. Kinkelin, H. Leppelsack, S. Liebald, D. Scholz, G. Carle, and D. Schupke, "Performance perspective on private distributed ledger technologies for industrial networks," in *2019 International Conference on Networked Systems (NetSys)*, 2019, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/document/8854512

[30] C. Wang and X. Chu, "Performance characterization and bottleneck analysis of hyperledger fabric," in *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)*, 2020, pp. 1281–1286. [Online]. Available: https://ieeexplore.ieee.org/document/9355625

[31] K. S. Su Wai, E. C. Htoon, and N. N. Myint Thein, "Performance evaluation of m/d/1 queuing model on hyperledger fabric," in *2020 International Conference on Advanced Information Technologies (ICAIT)*, 2020, pp. 36–41. [Online]. Available: https://ieeexplore.ieee.org/document/9261808

[32] I. Pittaras, N. Fotiou, V. A. Siris, and G. C. Polyzos, "Beacons and blockchains in the mobile gaming ecosystem: A feasibility analysis," *Sensors*, vol. 21, no. 3, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/3/862

[33] "Multichain," Visited March 2021. [Online]. Available: https://www.multichain.com/

[34] Z. Hintzman, "Comparing blockchain implementations," 2017. [Online]. Available: https://www.nctatechnicalpapers.com/Paper/2017/2017-comparing-blockchain-implementations

[35] M. Dabbagh, M. Kakavand, M. Tahir, and A. Amphawan, "Performance analysis of blockchain platforms: Empirical evaluation of hyperledger fabric and ethereum," in *2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/9257811

[36] A. Panwar and V. Bhatnagar, "Distributed ledger technology (dlt): The beginning of a technological revolution for blockchain," in *2nd International Conference on Data, Engineering and Applications (IDEA)*, 2020, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/9170699

[37] S. R. Niya, R. Beckmann, and B. Stiller, "Dlit: A scalable distributed ledger for iot data," in *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, 2020, pp. 100–107. [Online]. Available: https://ieeexplore.ieee.org/document/9274456

[38] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 583–598. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8418625

[39] "Ethereum upgrade." [Online]. Available: https://ethereum.org/en/eth2/