Contents

List of Figures

List of Tables

CHAPTER 1

Introduction

A sort description of the chapter.

1.1 Objectives

1.2 Contributions

1.3 Document Structure

CHAPTER 2

Background Review

In order to work on electronic bills of lading it is important to have an overview of several indispensable concepts. This chapter starts by providing a description of several essential security concepts necessary to understand blockchains. After this, the concept of blockchain is introduced along with its characteristics, usual organization and several concepts that distinguish them. Finally, with the intention of talking about the Bill of Lading a brief description of the shipping industry is presented.

2.1 Security Concepts

2.1.1 Public Key cryptography

The notion of public-key was proposed in a groundbreaking paper by Whitfield Diffie and Martin Hellman [1]. The authors proposed a public key cryptosystem where the problem of key distribution was extremely simplified, each user generated a pair of inverse transformations at his terminal. The deciphering transformation (now known as private key) should be kept secret and never communicated on any channel. The enciphering key (now known as public key) can be made public. Anyone can then use the public key to encrypt messages that only the owner of the corresponding private key can decipher. It is important to note that it is impossible (or very hard) to obtain a private key based on knowing the corresponding public key.

The main functions that public-key cryptography, or asymmetric cryptography, provide are: key establishment, non-repudiation, identification, and encryption [2].

- Key establishment protocols are used for establishing secret keys over insecure channels, one of these protocols is DHKE(Diffie-Hellman key exchange).
- Non-repudiation is the assurance that someone cannot deny the validity of something, refers to a service which provides proof of origin of data and integrity of the data, can be realized with digital signature algorithms, e. g., RSA, DSA or ECDSA.

- It is possible to identify entities through challenge-response protocols along with digital signatures.
- Messages can be encrypted using algorithms, for instance, RSA.

The major drawback is that the encryption is very computationally intensive with public-key algorithms, making it extremely slow when compared to symmetric ciphers. Therefore, data encryption with these algorithms is somewhat rare. Contrastingly, symmetric algorithms do not provide or make it exceedingly difficult to provide the functions of nonrepudiation and key establishment. Most practical protocols that need to use all the above functions are hybrid protocols, that is, incorporate public-key algorithms and symmetric algorithms to take advantage of the faster encryption of data.

Most relevant public-key algorithms can be divided into three major families based on the fundamental computational problem.

- Integer-Factorization schemes are based on the difficulty of factoring large composite integers. RSA is the most notable from this family.
- Discrete Logarithm schemes are based on the discrete logarithm problem in finite fields. These include Diffie-Hellman key exchange (DHKE), or the Digital Signature Algorithm (DSA).
- Elliptic Curve schemes are a generalization of the discrete logarithm algorithm. Examples of these are the Elliptic Curve Diffie-Hellman key exchange (ECDH) and the Elliptic Curve Digital Signature Algorithm (ECDSA).

All three of these families are based on number-theoretic functions that require arithmetic with very long operands and keys. Longer operands and keys provide more security.

Proposals outside these three families do exist but often lack maturity, have unknown robustness against mathematical attacks, or have poor implementation in some respects. Despite that, other schemes as effective and secure as the main schemes just have not reached widespread adoption.

2.1.2 Digital Signatures

Digital signatures are one of the most important cryptographic tools, along with key establishment over insecure channels they are the most important instance of public-key cryptography. They share some functionality with handwritten signatures, they can be used to assure that a message is authentic to the signer.

There are many security needs in digital signatures besides encryption and key exchange, therefore symmetric cryptography does not provide all the security functions needed.

Assuming two communicating parties, Alice and Bob, who share a secret key. The secret key is used for symmetric encryption. If Bob sends an encrypted message to Alice, and she decrypts a meaningful message, she can conclude that it was in fact someone with the secret key who sent a message. If only Alice and Bob have the key it is reasonable for them to assume that the message was not altered in transit. Having said that, even though Alice and Bob want to communicate securely between them, they also might be interested in deceiving each other. This is where symmetric-key schemes fall short, they do not protect the two

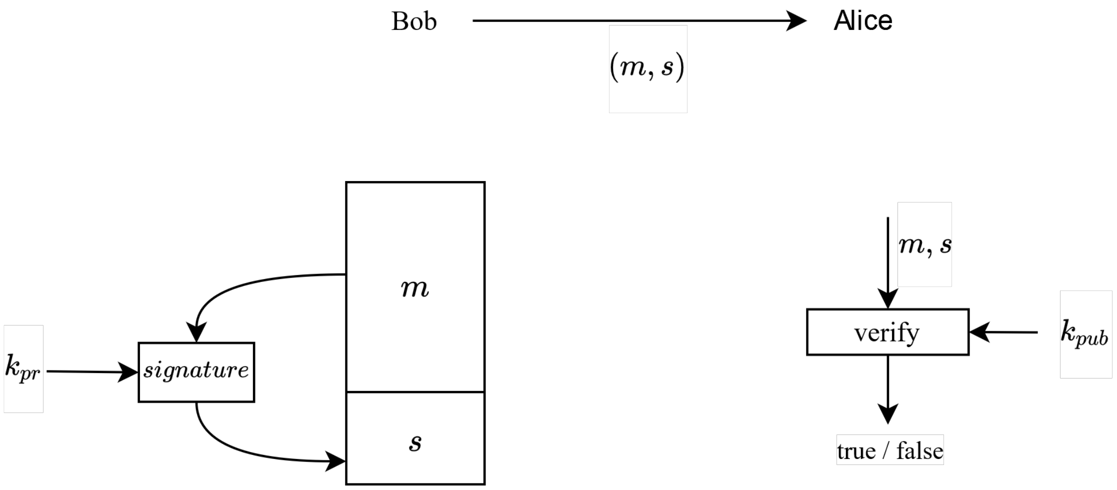


Figure 2.1: Digital signature process

parties from each other. An example of this would be if Alice signed a work contract with specific terms, and later Bob decided he was not happy with the terms and changed them the signed the contract again. There is no way for Alice to prove that the signed contract is no longer the one she agreed to.

There are many situations where it is necessary to prove to a neutral third party that one of the two parties generated a message, i. e. the third party can conclude without a doubt who generated the message even if all parties are dishonest. It is not possible (or overly complicated) to use symmetric-key schemes to solve this problem because Alice and Bob have the same knowledge (the keys), therefore the same capabilities, anything that one party can do, the other can too. Thus, a neutral third party cannot distinguish who performed a certain operation. A solution to this lies in public-key schemes.

The basic idea is that the person who signs the message uses his private key, and the person receiving uses the matching public key. The scheme shown in figure 2.1 depicts the process.

The process is started by Bob when he signs the message, m. The signature algorithm depends on Bob's private key, k_{pr}, assuming he keeps his private key private, only he can sign a message on his behalf. Since the objective of the signature is to sign a message, then the message itself is also an input to the signature algorithm. After the message is signed, both the message and signature, s are sent to Alice as a pair. The signature by itself is useless, it must be always accompanied by the message.

The signature will only be useful if Alice can verify it, this requires a validation function that takes both the signature and the messages inputs. To verify it was actually signed by Bob, it is also necessary his public key, k_{pub}. Since the only objective of the verification is to determine whether or not the signature is valid the only output is a binary statement, true or false.

A signed message can be traced back to the signer since a valid signature can only be computed with the unique signer's private key.

There are several security functions that can be achieved with digital signatures, the most important being:

- Confidentiality: information is secret for everyone except the authorized parties.
- Integrity: message has not been tampered with or altered.
- Message authentication: message has not been modified while in transit (integrity) and that the receiving party can verify the source of the message.
- Non-repudiation: the sender cannot deny the authenticity of its signature on a document.

This four functions can be achieved in a straightforward manner with public-key schemes. For confidentiality symmetric ciphers would be the primary option but one could use asymmetric encryption. Digital signatures and message authentication codes, introduced in section 2.1.3, provide integrity and message authentication. And finally, non-repudiation as discussed can be achieved via digital signatures.

2.1.3 Hashes

A hash function is a function that takes an input message of variable length (transformed in a string of bits) and produces a fixed length output. For a particular string of bits the result of the hash function, hash value or digest, can be considered a fingerprint of the string, this means that each input string should have a unique representation of itself. Hash functions have many applications in cryptography [3], some examples are presented next.

Password hashing

When a user wants to log on to a service the system needs to verify the correctness of the password presented by the user with the one stored. The obvious solution is to compare the password text directly, but if the stored password is not encrypted anyone that can access the system can steal the passwords.

With hash functions, a password does not need to be stored in the system, it can instead store the value of the hash. When a user provides the password, it can calculate the hash and compare it with the stored value. If they match the original passwords also match and the user may enter. Even if the hash password is somehow in the hands of an attacker, he cannot log with the hash value nor can he derive the original password from the hash value. There is still the danger of an attacker guessing (or using a list of common passwords) the password and comparing its hash with the original password hash especially if the password chosen is easy to guess.

Message integrity

Hash functions are often used to generate Message Authentication Codes (MAC), as the name suggests it is a piece of information used to authenticate a message, i. e. to confirm that the message came from the specified sender and was not altered. The MAC provides a guarantee of data integrity and authenticity when a message is sent in an insecure channel.

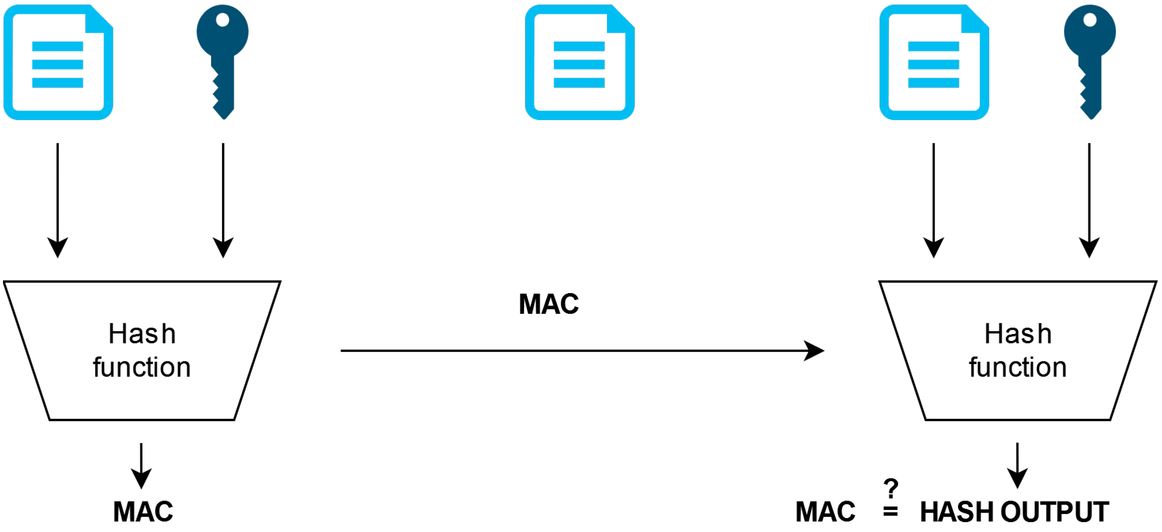


Figure 2.2: Message authentication code creation and verification

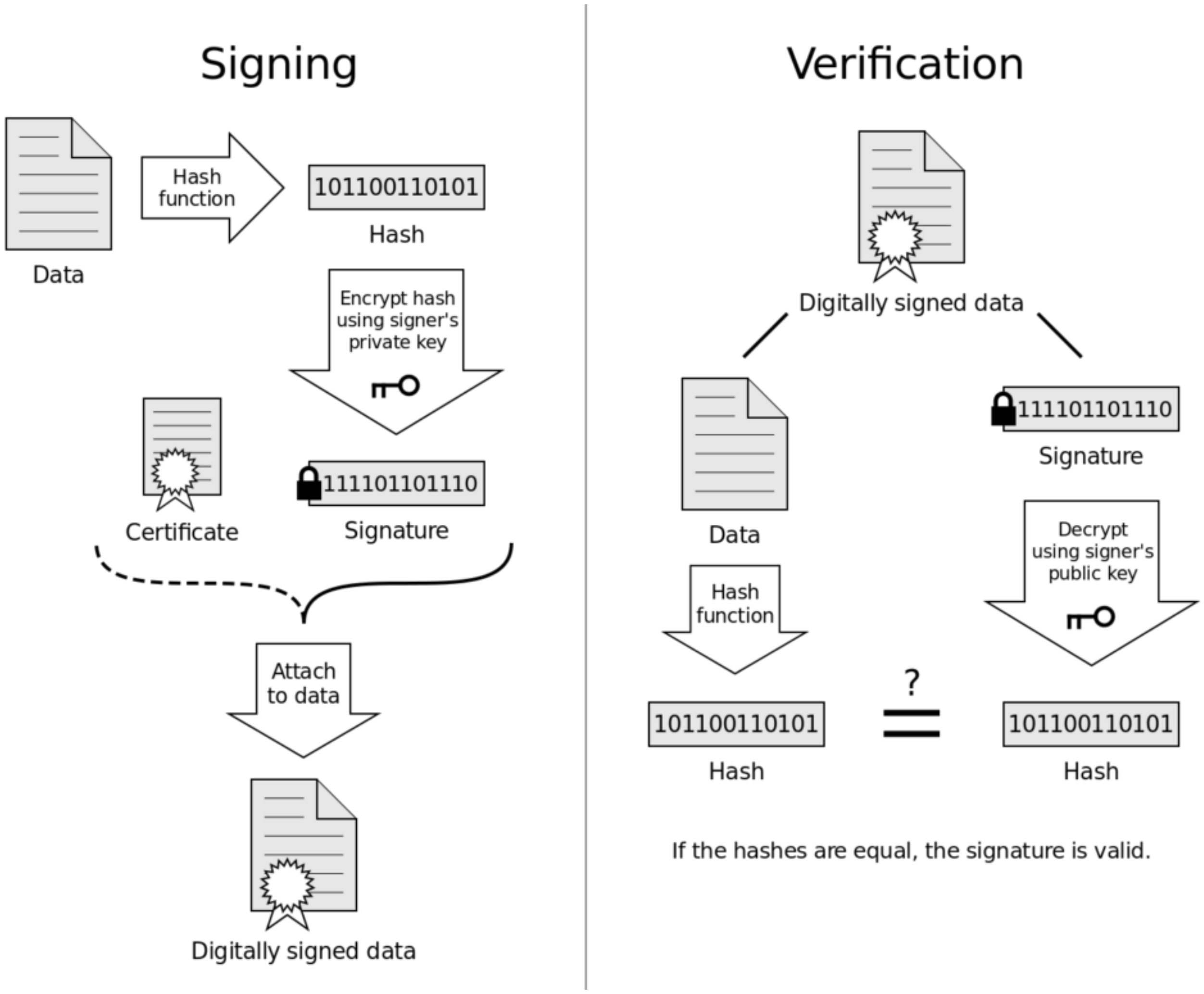
Sending only the hash of the message would not be secure because the hash function is known, an attacker could modify the message and generate a new hash.

If the sender and receiver have an agreed secret, the sender can use a hash function to generate a MAC for a message by concatenating it with the secret and computing the hash of the result, this is a keyed hash. The receiver can then do the same process and compare it to the received MAC, if the received MAC matches the one computed he can be confident that the message received was sent by someone with the secret and the message was not altered. This is illustrated in figure 2.2 where the key represents the common secret.

Digital signature efficiency

Since asymmetric algorithms have a limited message size, if the message is bigger than that limit it is not possible to sign the whole message at once. A solution would be to split the message into several parts, smaller than the limit size, and sign each part separately. However, this as some problems, as stated previously public key algorithms are computationally intensive and doing several signatures would take a long time to sign but also to verify, it could also lead to security problems since there is no protection to the whole message, just to each individual part.

In figure 2.3 we have good solution that would be to compute a hash value of the message and signing that instead of signing the message itself. Since hash functions are much less computationally intensive and the resulting hash value of the message is much shorter, the resulting time to create the digital signature is much smaller and the whole message is contained in a single signature.



Source: Center for Advanced Studies, Research and Development in Sardinia (CRS4) [4]

Figure 2.3: Digital signature with hash function

Properties

There are attacks that prey on the weaknesses of hash functions, the three main properties necessary for a hash function to be considered secure:

- Preimage resistance
- Second preimage resistance
- Collision resistance

The three properties are illustrated in figure 2.4.

A good hash function must be a one-way function: given a message m it is possible to compute $h(m)$, but given a value x it is computationally infeasible to find an m such that $h(m) = x$. In other words, the function cannot be inverted.

Second preimage resistance or weak collision resistance means that given an input m1 such that $h(m_1) = x$, it should be computationally infeasible to find any second input m2 that has the same output, $h(m_2) = x$. In a collision resistant hash function, it is computationally

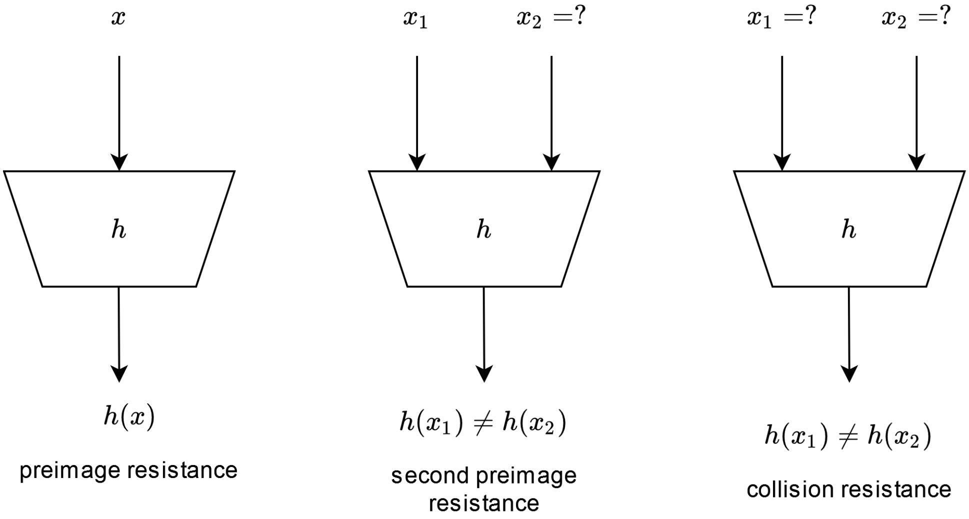


Figure 2.4: Hash function properties

infeasible to find two different inputs x1!=x2 with $h(x_1) = h(x_2)$. This is generally harder to achieve compared to weak collision resistance [5].

Even if a hash function is resistant to all these collisions it does not mean that there will never be a collision, it means that it should be computationally impractical to find any. The concept avalanche effect, if a small change is inserted into the input it should result in a totally different hash value, is desired in all hash functions.

Hash functions must have these three main security properties but should also have other practical properties. As stated above, they can be applied to messages of any size, produce a hash value of fixed length and all of this should be relatively easy to compute.

Nowadays, there are multiple categories and families of hash functions.

Message Digest

Message Digest (MD) functions were developed by Ronald Rivest. MD4 and MD5 are in this category, and both have been found to be insecure and are not recommended anymore. Both are 128-bit hash functions commonly used in file integrity checks.

Secure Hash Algorithms

The most common Secure Hash Algorithms (SHAs) are:

- SHA-0: developed by the U.S. Government Capstone project, was originally called SHA-1, produces a 160-bit hash value. Was withdrawn by the National Security Agency (NSA) and superseded by the revised version in 1995.
- SHA-1: introduced in 1995, and also a 160-bit hash function. It is commonly used in SSL and TLS implementations but is now considered insecure and is now discouraged in new implementations.

- SHA-2: this is a set of four functions named after the number of bits of the hash: SHA-224, SHA-256, SHA-384, and SHA-512. They are built using the Merkle-Damgard structure
- SHA-3: it is the latest family of SHA function, released in 2015, and supplies the same output sizes as SHA-2. SHA-3 is a standardized version of Keccak. The algorithm uses a approach called sponge construction instead of the Merkle-Damgard structure.
- RIPEMD: the acronym for RACE Integrity Primitives Evaluation Message Digest, is a family of hash functions based upon the design principles of MD4. RIPEMD has different versions including 128-bit, 160-bit, 256-bit, and 320-bit.
- Whirlpool: designed by Vincent Rijmen (co-creator of the Advanced Encryption Standard) and Paulo Barreto. It is a block cipher hash function designed after the Square block cipher. It uses a Miyaguchi-Preneel compression function. Whirlpool produces a hash of 512 bits [6].

2.2 Blockchain

In 2008, Satoshi Nakamoto, whose true identity is still unknown, released a whitepaper [7] that described "a peer-to-peer electronic cash system" with the name Bitcoin, he introduced the term chain of blocks. Satoshi Nakamoto remained an active developer in the Bitcoin community until 2011, when he handed over Bitcoin development to its core developers. The term chain of blocks evolved into the world blockchain. Bitcoin became the first ever conceptualized blockchain and also the biggest to this day. Blockchain has developed into one of the biggest ground-breaking technologies today, it has the potential to impact every industry from finance, supply chains to even art.

Blockchain can be seen as a large database that stores information of transactions securely and allows users to interact with others without the need of any trusted third party. Technically, the blockchain acts as a ledger that records and tracks resources without requiring a centralized trusted authority. It allows for the sharing of information between parties within a peer-to-peer network. Nowadays, the resources can material like money, houses, land, etc. Or immaterial like digital documents, digital art, intellectual property rights, etc. Blockchain provides a different way of storing data with a "chain of blocks" using cryptography to ensure integrity of the data stored.

The concept that is today known as blockchain, was started by Stuart Haber and W. Scott Stornetta with a paper [8], referenced directly in Satoshi Nakamoto's Bitcoin paper, titled "How to time-stamp a digital document". In the paper it is proposed a solution to time-stamp digital documents through a chain linking documents together, and each document's certificate would contain a link to the previous document in the chain.

Blockchain is a network of nodes connected over the internet, any device connected to the internet with an IP address can be a node in the blockchain. Since it is a distributed network, all nodes are equally important, but may have different roles in order to make the blockchain work properly. A node can store information that is on the blockchain or a copy of all the information recorded. Nodes can also process transactions, place them in blocks, append them to the blockchain, approve them, and finally send them to the network.

2.2.1 Distributed Systems

Blockchain is a distributed system at its core, it is a distributed leger which can be centralized or decentralized, even though it was originally intended to be a decentralized platform. It can be considered a decentralized-distributed system since it contains properties of both.

A distributed system is a collection of two or more nodes that work together in a coordinated fashion to achieve a common goal. All these distributed nodes have one shared state and operate concurrently. These systems are modeled in such a way that end users see it as a single platform.

A node can be seen as a single entity in a distributed system. All nodes are interdependent, and autonomous and linked by a network to share information and communicate between each other. Nodes can be honest, faulty, or malicious. One that exhibits irrational behavior is known as a Byzantine node after the Byzantine Generals Problem [9].

The inconsistent behavior of Byzantine nodes can be intentionally malicious, therefore detrimental to the operation of the network.

Byzantine Generals Problem

The Byzantine Generals Problem is a classical problem faced by distributed networks, first theorized by Leslie Lamport, Robert Shostak, and Marshall Pease, the authors of the paper with the same name. Solving it was a key development for the creation of blockchains.

The problem consists of a group of generals, that lead distinct parts of the Byzantine army, deciding whether to attack or retreat from a city. They communicate with each other via messengers and need to agree upon a common plan of action. However, some of them are traitors trying to prevent the loyal generals from reaching an agreement. This calls for an algorithm that guarantees that all loyal generals decide on the same plan of action, and a small number of traitors cannot cause the others to choose a bad plan. As an analogy to distributed systems, the generals are the nodes, the traitors are Byzantine (faulty) nodes, and the messengers are the channel of communication.

In 1999 by Miguel Castro and Barbara Liskov described a new state-machine replication algorithm, Practical Byzantine Fault Tolerance (PBFT), that can tolerate Byzantine faults and can be used in practice [10].

2.2.2 Properties

A good technical definition for blockchain is that it is a “peer-to-peer, distributed ledger, that is cryptographically secure, append-only, immutable, and updateable only via consensus or agreement among peers” [11]. To understand this definition, it is important to understand some of its properties.

From all blockchains developed it is possible to identify common properties in most of them that make it suitable for many applications in different industries. The most important are presented below.

Peer-to-peer

It refers to networks that use a distributed architecture. All members of the network are referred to as peers, each peer in a peer-to-peer network is equal to other peers and each has the same rights and duties as others. Peers are both clients and servers at the same time.

Distributed

A distributed ledger can be described as a ledger of any transactions, maintained in a distributed form across the network among all peers in the network. More on distributed systems in section 2.2.1.

Decentralized and Updateable via consensus

Since in a peer-to-peer network peers are all equal to each other, there is no central authority. In a centralized transaction system, a mediator is necessary to provide the transaction services. An example of this is a bank, it acts as a central authority and everything has to go through it; this gives the central authority full control of the system. Decentralization is the transfer of control and decision-making from the central authority to a distributed network [12] (section 2.2.1). Without a central authority, it is necessary to have a consensus mechanism so different network nodes can validate transactions. Any update made to the blockchain is validated and added only after consensus is reached among all participating peers. In order to achieve this consensus, there are different consensus algorithms which ensure that all peers agree about the final state of the data.

Cryptographically secure

A cryptographically secure ledger uses cryptography to provide security services. These services include non-repudiation, data integrity, and data origin authentication.

Anonymity

Any user in the network can communicate with other users using their public address, much like explained in public key cryptography, it is not possible to identify a user using its public address. Therefore, even though the system is transparent, the anonymity of the user is maintained.

Transparent

All transactions in a blockchain are public and visible to anyone who is a part of the network, a network participant can access holdings and transactions of public addresses, this is what makes the blockchain transparent [13]. This type of transparency never existed in centralized systems.

Persistency

When validating transactions, it is possible to identify invalid transactions and stop them from being inserted into a block. Once transactions are connected to a block, it is not possible to remove or reverse them. There are some legitimate motivations to remove data once it has been added, such as the right to erasure ('right to be forgotten') defined in the General Data Protection Regulation (GDPR) [14].

Append-only and Immutable

Data can only be added to the blockchain time ordered. This property implies that once the data is added to the blockchain, it is almost impossible to change it and can be practically immutable. There are rare scenarios where data can be changed, when there is collusion against the network and 51 percent of the power is obtained by an organized group.

Anonymity

Any user in the network can communicate with other users using their public address, much like explained in public key cryptography, it is not possible to identify a user using its public address. Therefore, even though the system's transparent the anonymity of the user is maintained.

2.2.3 Block Structure

A block is a set of transactions bundled together and connected with each other. A transaction is a record of an event, in the case of Bitcoin, it is a transfer of value between Bitcoin wallets. The size of the block depends on the type and design of each blockchain.

What creates the chain of blocks is the fact that each block has a reference to the previous, except the genesis block. The genesis block is the only hardcoded block and is the first one in the chain, therefore it does not reference another block. The structure of the blocks also varies depending on the type and design of the blockchain. However, there are a few essential attributes for the overall functionality of the block. The block header contains the reference to the previous block, timestamp, nonce, and Merkle root. The block body contains the transactions. These are always present in a block and each blockchain will have other attributes necessary for the specific implementation. Some of these elements are self-explanatory but others are not.

A nonce, number only used once, is a random number generated for specific uses, that vary with time to make sure they cannot be reused. For these reasons, they are used in several cryptographic operations to grant replay protection, authentication and encryption. In blockchains, it is essential for transaction replay protection and also for Proof of Work consensus algorithms.

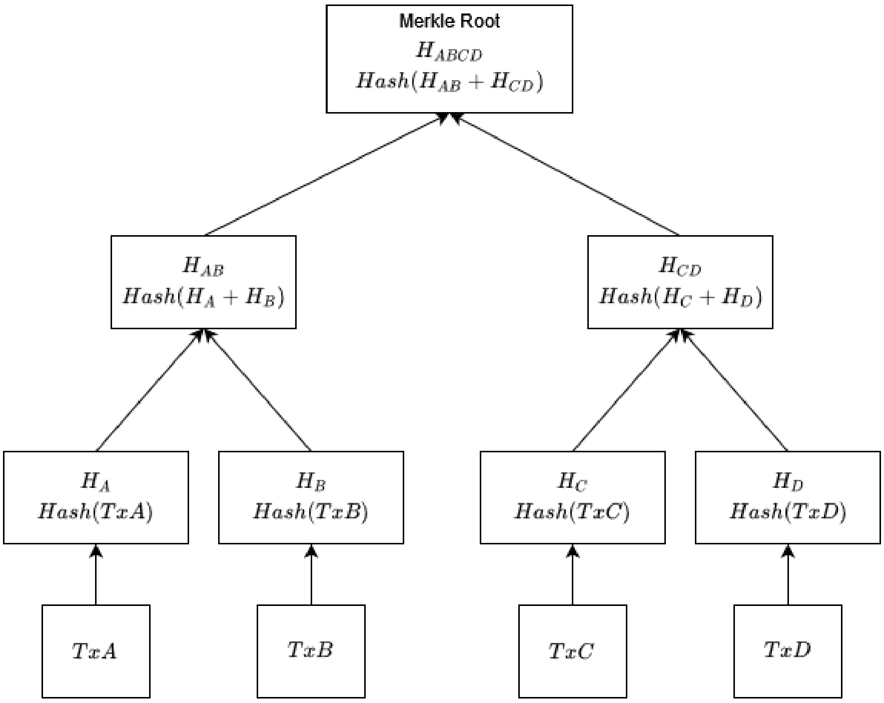


Figure 2.5: Merkle tree of transactions on leaf nodes

To know what a Merkle root is, it is important to know what the Merkle Tree is. The Merkle Tree was invented in 1988 by Ralph Merkle, the original paper [15] described Merkle trees in the context of digital signatures but, nowadays it has a much broader set of applications. They are extensively used to validate large data structures. Taking transactions in a block as an example, they would be the leaf nodes of the tree maintaining their order from the block, for each leaf node the hash of the transaction is calculated. Every internal node (a node that is not the root or a leaf node) of the tree combines the hashes of its children and calculates the resulting hash, this process is continued until the root of the tree, the Merkle root. This is evident in the figure 2.5. Basically, the Merkle root is the hash of all transactions in the block. This means that any change in a single transaction (Tx) will change the Merkle root, and consequently this will help to find whether a transaction in a block is tampered with without having to verify every transaction one by one.

A visualization of the structure of a generic blockchain block and the connection between different blocks is presented in the figure.

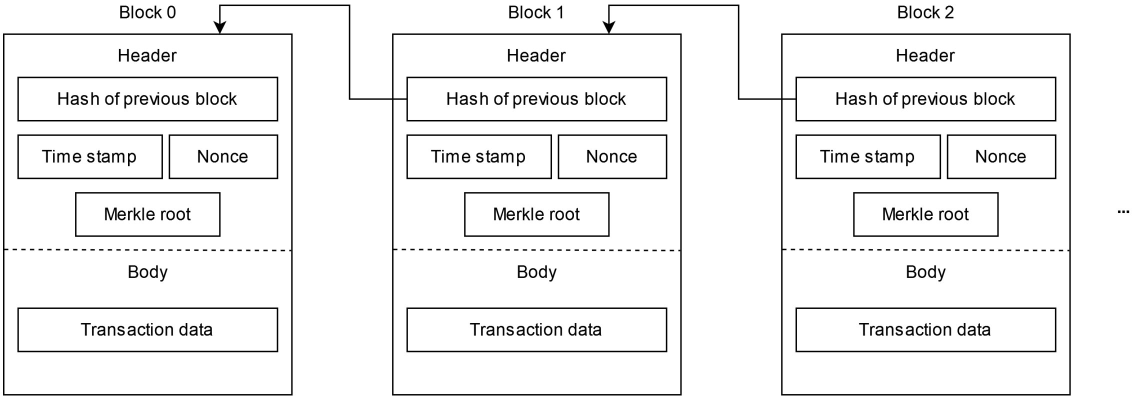


Figure 2.6: Block structure and connections

2.2.4 How blocks are accumulated

After understanding what blocks are and how they are structured it is important to know how blocks are created and accumulated in the blockchain. Five main steps are identified [11]:

- A node starts by creating a transaction and digitally signing with its private key. This transaction can represent a few actions, most commonly the transfer of value between users. A transaction data structure depends on the blockchain but usually consists of some logic of transfer of value, relevant rules, source and destination addresses, and other information to help in validation.
- A transaction is propagated with the use of a flooding protocol, Gossip protocol, to nodes that validate it based on existing criteria. Usually, more than one node is required to validate the transaction.
- After the transaction is validated, it is included in a block, which will then be propagated onto the network. After this, the transaction is confirmed.
- This newly created block becomes a part of the ledger and the next block created will cryptographically link itself to this block, its parent block. The link created is a hash of the parent block. At this point, the transactions inside the block are confirmed twice and the block gets its first confirmation.
- Every time a block is created transactions are reconfirmed.

2.2.5 Blockchain types

In this section, different relevant types of blockchains will be analyzed from a technical and business perspective.

Distributed ledger

Before defining different types of blockchains it is important to understand the concept of distributed ledger. A distributed ledger is a broad term used to describe shared, distributed databases, it encompasses all sorts of structures, such as the blockchain, which is just one type of distributed ledger.

Blockchains have two additional distinguishing factors from all other types of distributed ledgers. The data is organized in a block structure and it has a particular sequence. In order to keep the blockchain ledger growing, data is stored in a block and it is attached to the previous block maintaining a sequence. There are technologies using block structures that are often called blockchains due to the popularity of the term, but this is not enough to call it a blockchain, the sequence of data is also necessary. The important takeaway is that all blockchains are distributed ledgers, but not all distributed ledgers are blockchains.

Permissioned Blockchain

A permissioned blockchain can be seen as an additional security system, as they maintain an access control layer in order to permit only well-defined identities to transact with the distributed ledger in the network. They allow for different levels of permissions to be designated to its users, therefore, satisfying confidentiality needs. These blockchains may allow anyone to transact in the network once their identity and role are defined. Such Blockchains are better fitted for individuals who within the blockchain need to define security, identity, and role.

Public Blockchain

A public blockchain is a blockchain where users can join whenever they want, there are basically no restrictions when it comes to participation. Users can see the ledger and take part in the consensus process. Thus, all transactions over public blockchains are transparent. They may or may not be rewarded for their participation. They are also permissionless as anyone is allowed to maintain a copy of the ledger on their local nodes and participate in block validation.

Private Blockchain

A private blockchain is a permissioned blockchain, therefore participants need consent to join the network. Only those allowed to join the network can view the transactions. Private blockchains are considered more centralized than the public counterpart because the entities responsible for the blockchain have more control over the participants and governing structures, therefore are more suitable for individual enterprise solutions.

There is no transfer of currency or tokens in these blockchains, also no transaction fee is necessary since the nodes involved in the validation of the block are well known and trust each other. It is also possible to rollback in a private blockchain if necessary.

Consortium Blockchain

Like private blockchain, consortium blockchain, also called hybrid blockchain, also requires permission for participants to join the network. On the contrary, the network is not restricted to a single organization or enterprise, it expands to multiple organizations and provides accountability between parties involved. Transaction fee is also not necessary in consortium blockchain. It has the privacy benefits of a private blockchain while maintaining the secure

Property	Public Blockchain	Consortium Blockchain	Private Blockchain
Members of the consensus mechanism	All nodes	Selected nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible to tamper	Can be tampered	Can be tampered
Efficiency	Low	High	High
Centralization	No	Partial	Yes

Table 2.1: Comparison between public, consortium and private blockchains

and transparent nature of public blockchains. The table 2.1 shows a comparison between public, private and consortium blockchains similar to the one in a study by Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang [16].

Tokenized Blockchains

These are the standard blockchains, they generate cryptocurrencies as a result of the consensus process via mining or initial distribution. The main examples of this type of blockchain are Bitcoin and Ethereum.

Tokenless Blockchain

Tokenless blockchains are designed so that they do not have the basic unit for the transfer of value. These are still valuable when there is no need to transfer value, only sharing data among different trusted parties is required.

2.2.6 Smart contracts

The concept of smart contracts was first introduced by Nick Szabo [17]. They are enforceable and automatically executed programs that run on top of the blockchain and have business logic to be executed in certain conditions. This feature is not available in all blockchains but has become a desirable feature, since they provide flexibility and power to the blockchain applications.

Smart contracts were popularized by Ethereum, the second biggest blockchain, smart contracts allowed decentralized applications (dApps) to be built on the network. A smart contract can be divided into a few steps. First, it needs an agreement between two or more parties. Then, conditions have to be agreed upon to know when the smart contract will be completed, this decision is then automatically written on the blockchain, becoming immutable and irreversible. Once the contract is completed, the transaction is recorded on the blockchain just like any other would.

What makes smart contracts a desirable feature is not just as a contract for a payment, there are innumerable implementations that can automate several parts of a society. Some examples of where they can be applied are, for example, real estate, insurance, supply chains, digital identity, banking, and many others.

2.2.7 Consensus

One of the most important aspects in a blockchain is the consensus, the choice of the consensus algorithm is highly dependent on the type of the blockchain. Some consensus algorithms are not suitable for distinct types of blockchains; therefore, it is essential to choose an appropriate algorithm for a certain blockchain.

Consensus is the process of agreement between nodes that do not trust each other on the final state of the data. In a client-server architecture it is simple to achieve consensus between client and server, but in distributed systems several nodes must agree on a single value, making it quite challenging to achieve an agreement. This process of obtaining an agreement in a common state or value between several nodes, despite failure of some of them, is known as distributed consensus.

To achieve consensus there are a few requirements that must be met. These requirements are:

- Agreement: All honest nodes, or non-malicious, should agree on the same value;
- Termination: All honest nodes must reach a decision and terminate the consensus process;
- Validity: The final value agreed upon by all the honest nodes, should be one proposed initially by at least one of those honest nodes;
- Integrity: Every node can make a decision only once in a single consensus cycle.

Consensus mechanisms can be divided differently depending on the criteria used. A reasonable categorization is presented below:

- Proof-based, or leader-election based, where a leader is elected randomly and proposes a value. It can be also referred to as fully decentralized or permissionless;
- Byzantine Fault Tolerance (BFT)-based, an approach based on rounds of votes, they are also known as consortium or permissioned mechanisms.

Typically, BFT-based consensus mechanisms perform very well when there are few nodes, contrasting with leader-election lottery-based mechanisms that performs much better with a large number of nodes. BFT-based consensus mechanisms do not scale as well as leader-election lottery-based mechanisms, but these also perform much slower than their counterparts. Therefore, when choosing consensus algorithms, it is important to keep in mind the type of the blockchain and what balance between scalability and performance is better suited.

Nowadays, there are several different consensus algorithms in the context of blockchain and others are being researched. It would be boring to list them all, but the most notable are in the following list:

- Proof of work (PoW): Currently, the most widely used and one of the most robust mechanisms in blockchain. The so called miners compete to find a nonce that produces a hash with a value lower than or equal to that set by the network difficulty, as evidence that they have expended computational power in order to achieve consensus. This process is referred to as mining. It is extremely robust against collusion attacks, where different nodes cooperate to deceive the blockchain, if 51% of the nodes of the blockchain collude, they will effectively decide which blocks are added to the blockchain. This mechanism is used in blockchains like Bitcoin, Ethereum [18] and others.

- Proof of Stake (PoS): It is considered the substitute approach for PoW since it requires less computational power. In PoS, the creator of a new block is chosen in a deterministic way based on its wealth, commonly called as stake. A user that wants to attack the network has to invest in it to the point that it would outweigh the benefits obtained from the attack. Proof of Stake was introduced by Peercoin [19], but currently there are many applications, Cardano [20] being the most promising along with the upgrade to Ethereum that will eventually transition the network to PoS [21].
- Delegated Proof of Stake (DPoS): This is an innovation over PoS, where users with a stake in the system do not validate the blocks themselves but select delegates to do it for them. The selected delegates are changed periodically and have an assigned order to deliver blocks. Less delegates allow them to organize themselves efficiently and assign time slots to each delegate. Missing the blocks regularly will make the users vote to replace them for another delegate. This mechanism is used in the EOSIO [22] and TRON [23] blockchains.
- Proof of Authority (PoA): An alternative consensus mechanism that relies on well known and reputable validators to produce blocks. Validators are known entities that put their reputation on the line for the right to validate blocks. It is ideal for providing a control environment for testing features, some of Ethereum's testnets use this mechanism [24]. The most relevant use of this mechanism is in the VeChain blockchain [25].
- Proof of Importance (PoI): This idea is similar to PoS, differing on how users are evaluated. In PoI other metrics besides the size of the users stake in the network is used to choose the creator of a new block. These metrics include the net transfers, currency vested (not all the currency owned by a user is vested, it depends on how long it is in the user's wallet) and involvement in cluster of nodes. Users are rewarded for making transactions encouraging decentralization. This mechanism was introduced by NEM [26], and it is still the biggest blockchain using it.
- PBFT: It is a voting-based algorithm that is Byzantine fault tolerant, guaranteeing that the consensus mechanism is carried out even with the presence of nodes that exhibit irrational behavior (Byzantine nodes), as long as some nodes are working and behaving properly. A primary node produces candidate blocks that are voted on by the secondary nodes, this primary node, the leader, is changed in a defined order. Many messages are sent to achieve consensus, commit blocks and maintain a healthy leader node. This makes PBFT a leader-based and network-intensive mechanism. An example of blockchain that uses this mechanism is Hyperledger Sawtooth [27].
- Proof of Storage (PoS): This scheme is based on the outsourcing of storage capacity. The nodes that outsource storage, the prover, show to the verifier that the storage is actually used to store a piece of data at the time in a challenge. Proof of Storage is used

in Filecoin [28], and several variations of this scheme have been proposed and used in many blockchains, like Proof of space-time being used in the Chia network [29].

- Proof of Capacity (PoC): Emerged as an alternative to PoW high energy consumption. PoC works by, instead of repeatedly change the nonce and hash for the solution value, it stores possible solutions in a list on the node's hard drive even before starting to mine. The larger the list stored, the more chances to have the required hash value. An evolution of this scheme, Proof of Commitment, is used in Burstcoin (changing to Signum network) [30].
- Proof of Elapsed Time (PoET): Every participant node in the network generates a random time to wait and sleeps for that duration. The one that wakes up first, which is the one with shortest wait time, commits a new block to the blockchain. In this mechanism it is necessary to ensure that the nodes select the time randomly and not maliciously choose a smaller duration in order to have a higher chance of winning. It also must ensure that the node that wins has in fact waited for the duration randomly generated. This mechanism was introduced by Intel, that also contributed to the development of the blockchain Hyperledger Sawtooth [31].

2.3 Shipping industry

Ever since history has been recorded, humankind has used watercraft for communication, travel or trade. Trade first began between tribes, but with the rise of nations and empires, trade routes and ports were created. With the creation of bigger and more robust vessels, new ports were successively founded and new trade routes created.

With the advent of steam power in the 1820s, ships became independent of the wind and much more robust against adverse weather. It also enabled the timetabling of services as steam was much more reliable and vessels were larger, scheduled services started to appear in most main routes.

Nowadays, 90% of the world's goods are transported in the shipping industry. And has become the most affordable means of transportation in international import and export.

2.3.1 Containerisation

For centuries, the methods for handling of cargo remained unchanged. Different types of goods were handled individually and stowed manually in place. In the late 1950s and early 1960s there were several attempts to "unitise" cargo in pallets or large bundles in order to speed up cargo handling, but these attempts did not provide the wanted results. The introduction of containers with standardized dimensions in the 1960s was the optimal solution, it can be used in all general cargo movements. Container transportation requires specific ships and port facilities with special cranes, storage space and railway systems. Since this required an initial substantial investment, it started in the main trade routes and soon expanded worldwide to become one of the main drivers of globalization. Nowadays, using standardized containers allows for huge savings, since the goods only need to be packed once and can be transported in different modes of transport - ship, rail or truck. The time saved by avoiding unpacking and repacking reduced costs of port charges and stowage, and possible demurrage costs. Additionally, the containarisation substatially reduced the cost per tonne-mile between ports.

2.3.2 Sale of goods

Buying and selling goods involves the creation of a contract or agreement between the two parties involved, one that is selling the goods and the other accepting to buy the goods in exchange for something called consideration. Usually, the party selling the goods requires money, and the party buying the goods requires the goods themselves. This is a simple process when the exchange is made within a country where one can use credit cards, money, checks or other forms of payment. However, with international transactions, it is different due to:

- The distance between countries;
- The large sums of money usually involved in the shipping industry;
- The difference in legislation and difficulty of enforcing legal remedies in other countries.

Transfer of funds between countries

The difficulty of sending money from one country to another varies considerably with the countries involved. Some countries apply no barriers, while others have extremely strict exchange control. When there is no control, there are a few different methods. The simplest is a check or banker's draft that can be drawn on the payer's bank in its own currency, the payee's bank sells the currency in which the check is drawn and credits the account deducting charges for providing the service. Another better method is credit transfer, the charge the bank makes is dependent on the speed of transfer required. A big advantage over the check is that the charges do not have to necessarily fall upon the payee.

Methods of payment in international trade

When buyer and seller belong to the same group of companies, or when the merchants know and trust each other, they can use open account trading and use the methods of transfer mentioned in the previous section. But the question of when payment should be made remains.

The two parties always want to hold on to the money for as long as possible, but it is not possible to satisfy both. The seller, or shipper, would prefer to receive the money with the order, but the buyer would rather pay on delivery. In all methods of payment the Bill of Lading is a requirement, this is a legal document that details the type and quantity of goods, destination among other information about the shipment; it is also a document of title, a receipt for the shipped goods and a contract between carrier and shipper containing clauses (more on the Bill of Lading later on Section 2.3.5). With open account trading, a usual method is payment against documents, this requires the seller to send the invoice and Bill of Lading as soon as the shipment initiated, and the buyer will preform the payment once the documents are received.

Bills of Exchange

This is a method of payment more secure than open account trading. In this method a document is prepared, similar to check but distinct in most cases, since it specifies that the payment is to be made in a future date.

This method allows both parties to maintain their cash flow to the maximum, the buyer will only have the payment debited on the specified date and the seller may choose either to wait or to negotiate with another party in order to sell the bill at a slightly smaller value, this process is called discounting a bill of exchange [32]. If the seller agrees to the discounting charge when negotiating the sale of goods, both parties can conserve their cash flow without any of them being penalized.

Documentary credits

Can also be called letter of credit in the shipping context. The process to use documentary credits starts when both buyer and seller agree to a sales contract using this method of payment. The buyer instructs his bank, the issuing bank, to open the credit in favor of the seller. The issuing bank will then ask the sellers bank, or confirming bank, to confirm the credit. After, the confirming bank will inform the seller that the credit was issued, as soon has this happens and when it is satisfied that it can meet the terms, it may load the goods and dispatch them. Then, the seller sends documents covering the shipment to the confirming bank, that will then check the documents against the credit, and, if all is in order, will pay the seller according to the terms of the credit. The confirming bank sends the documents to the issuing bank, that will also check the documents and reimburses the confirming bank if all credit requirements are met.

This method is the most frequently used for payment of long-distance commerce and since documentary credits have several types (e.g. irrevocable, confirmed, silent confirmation, revolving, transferable,etc. [33]) the seller should stipulate that the payment shall be via a confirmed, irrevocable documentary credit. A confirmed documentary credit is usually requested when the seller has concerns with the ability of the bank to honor the credit, protecting the seller in case of situations like bankruptcy of the buyer or his bank, in this case the confirming bank will pay the seller. An irrevocable documentary credit means that the credit can only be cancelled with the agreement of both the seller and the confirming bank.

The confirming bank always compares the documents thoroughly with the instructions provided by the issuing bank. It has to obey its instructions to the letter, if there is even a slightest variation between the confirming bank's instructions and the documents presented by the seller it will cause the payment to be refused. Therefore, anything endorsed on the Bill of Lading that resembles a clause will result in the bank refusing to pay. The face of the Bill of Lading must describe the goods in the exact same wording the shipper requires in the credit.

To attenuate problems there is a close collaboration between major banks and the International Chamber of Commerce to create and revise a document called “Uniform Customs and

Practices for Documentary Credits,” currently in the sixth edition; therefore, it is abbreviated to UCP 600.

Documentary credits have an expiry date after which they become null and void. It may also have stipulations about the latest shipment date which is usually before the expiry date. Sellers may occasionally encounter delays in manufacture and will be arranging shipment very close to the final shipment date or expiry date. It will be problematic for the seller if the goods arrive at the destination port after the shipment date has passed or, even worse, the goods are still in transit but the credit has expired. The shipper’s money is tied up to the goods and it has title to the goods through the Bill of Lading but no immediate way to obtain payment. A shipper may request to obtain from the liner operator, or its agent, a Bill of Lading that falls within the expiry date of the credit. A letter of indemnity might be offered in exchange for that document, known as pre-dated Bill of Lading. This practice is fraudulent and a liner operator fulfilling such requests would be guilty of condoning fraud against the buyer and the bank. The Internal Group of P & I Clubs has made it clear to members that cover is withdrawn if the carrier is guilty of these malpractices.

2.3.3 Merchants

The expression merchant is used widely in different entities.

Shipper

First name and address in the Bill of Lading. An especially important person to the liner in terms of business but also important legally. The shipper is one of the two necessary identifiable parties in a contract, the carrier is the other.

It is not necessarily the one that delivers the goods to the port, for example, if the shipper purchases the goods from a manufacturer that will deliver the goods to port but does not appear on the Bill of Lading.

The shipper may disappear from the picture very quickly, if the sale is Free on Board (FOB); its job is finished as soon as the goods cross the ship’s rail and the ship is in charge of the goods on the consignee’s behalf. In a Cost, Insurance & Freight (CIF) sale, once the goods are shipped and the Bill of Lading is endorsed and sent to buyer or bank, the shipper will no longer play an essential role.

Forwarder

A forwarder may have distinct roles, it may be an agent for the shipper as far as the export customs entry but also when lodging bills of lading with the exporter as the shipper. If the forwarder undertakes the transport of goods from the manufacturing place to the docks, it can be, technically, a contractor, this is to say, a carrier instead of an agent in that part of the transport.

Forwarders often take on more duties as contractors, including booking of cargo, negotiating concessionary rates or rebates when available, and arranging road, rail, or other types of transportation to the port. Usually, the port of exit is decided by the forwarder.

They play a vital role at the discharging port when it is necessary expert knowledge to avoid delays in clearing customs. It may be the one to apply to the liner for the release of cargo, making it vital that the Bill of Lading is correctly endorsed by the consignee to allow the cargo to be released to the forwarding agent.

NVOCs or NVOCCs : Non-Vessel Operating (Common) Carrier

A NVOC presents itself as a carrier to specific destinations, and may accept to carry goods from other forwarders if possible. NVO(C)C has no precise legal standing, it is the Bill of Lading that determines the contract and it is crucial that the identity of the contracting carrier is clear, this is stated in UCP 600, Article 20, clause a [34].

Consignees and Endorsees

If a Bill of Lading is made out to the order of a consignee and someone different is to collect the cargo, then the consignee has to endorse the bill to the one collecting. There is no limit to the number of times a Bill of Lading can be bought and sold, as long as it is correctly endorsed each time. This means that a consignee that sells a Bill of Lading is also an endorsee.

Notify Party

When a documentary credit is involved, the consignee box is filled with the words ‘To order’ and below that the name and address of the notify party. Usually this is the actual consignee that cannot assume that role until payment is made and the Bill of Lading is sent by the bank that issued the letter of credit.

This party has no legal status under a Bill of Lading and, the liner has no obligation to communicate with the entity named in that box. However, for commercial reasons, all liners assume that obligation.

2.3.4 Insurance

Since ship owning involves high values and usually also the cargoes being transported, it is common that the ship is insured by the owners and the cargo to be insured by the shipper or the consignee. Marine insurance is a specialist business offered by several companies, the most famous being not a company but a kind of market, called Lloyds of London. In its origins merchants were willing to take some of the marine risks and for a payment of a premium would pay an agreed amount if the ship or the cargo was lost, usually each merchant only accepted a proportion of the risk by signing a policy one under the other. This is where the word underwriter appeared. Nowadays, underwriters are approached by insurance brokers seeking a percentage of the risk much like in its origins.

“P & I” Insurance

To cover unquantifiable risks, for instance, claims against the ship for damaged or lost cargo; or claims by third parties for damage to other ships, shore installations and injuries or loss of life, shipowners created clubs formally known as Protection and Indemnity Associations. This clubs are entirely owned by shipowners or members, but the running of the clubs is undertaken by firms or independent managers. Claims are paid out of funds subscribed by members, designated as calls, and additional calls may be made if claims exceed funds available.

2.3.5 Bill of Lading

The movement of goods between countries has always risen the problem of ownership: who owns the goods when they are being transported from the seller to the buyer? Therefore, a document that could provide evidence of ownership of goods and proof of the contract of carriage was necessary.

Brief History

The history of the Bill of Lading was contemporaneous with that of the carrier [35]. There is clear evidence of the use of a similar document to a Bill of Lading in the Roman empire. But, the modern Bill of Lading, as we know it today, originated in the eleventh century with the rise of great commercial cities in the Mediterranean. With problems arising between shippers and ship masters as to what goods were delivered, the need for an unquestionable proof also started to appear. Cities started to pass statutes that required every master to take a clerk obliged to take an oath of fidelity, and to enter in a register a record of the goods received from the shipper. In the fourteenth century another statute was introduced, which stated that if the register was at some point in possession of someone but the clerk, nothing it contained should be believed.

Until this the Bill of Lading did not exist, it was a book. The bill started to appear as a result of a statute that required clerks to give a copy of their registers to those who have the right to demand them, the master or owner.

In the sixteenth century the Bill of Lading started to appear in a form similar to the existing today. Toward the end of the century the use of the Bill of Lading as widespread. In the early seventeenth century a statute passed in France defined the Bill of Lading as an acknowledgment, given by the master, of the quantity of the goods loaded and also required marks of the merchandise, condition, name of the consignee and the amount of freight. Also, three copies should be issued, one for the shipper, one for the master and one to be sent to the consignee via another ship. Later, for a bill of a lading to be accepted as evidence it would have to be executed by a public notary instead of a clerk.

There was no statute law relating to bills of lading until mid nineteenth century. In 1855 the British Parliament passed the Bill of Lading Act, and most other countries engaged in international trade later adopted similar legislation. This act established the three functions of the Bill of Lading:

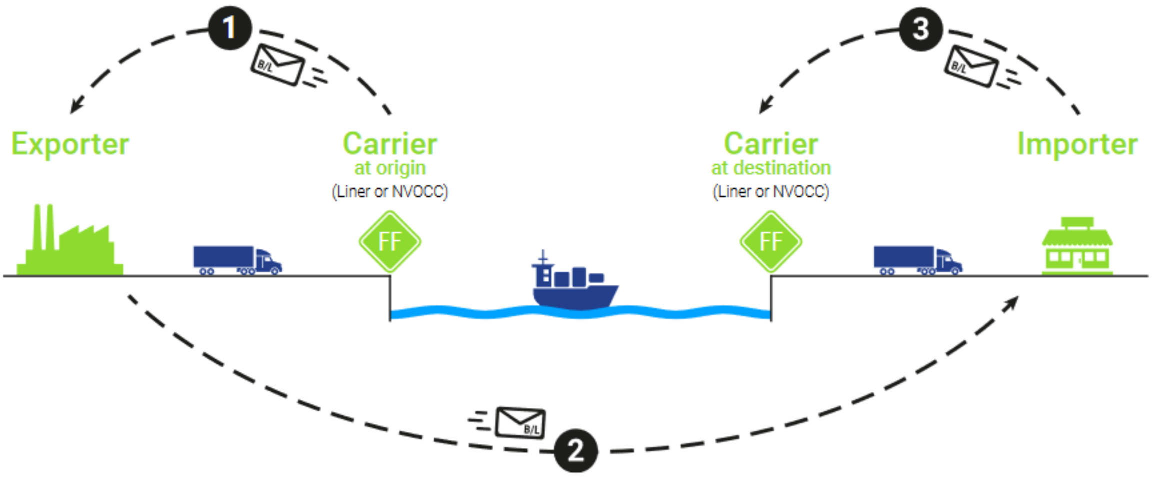
- Receipt for goods: When a carrier issues a Bill of Lading, it is confirming that goods have been loaded onto the transporting vessel. The receipt covers quantity and apparent quality of the cargo.
- Evidence of Contract of Carriage: The reverse of the Bill of Lading contains evidence of a ‘contract of carriage’ and may contain terms and conditions which are the whole contract. It is only ‘evidence’ because the Bill of Lading is only issued when the goods are received by the carrier, but the agreement of the transportation of goods would be already made at that time that is the moment the contract is established.
- Document of Title: As soon as the Bill of Lading has been signed for the carrier, the consignee can claim the goods as soon as they arrive at the destination port. If the consignee so wishes, he can endorse the Bill of Lading transferring the right – the title to the goods – to another party, as stated in the Bill of Lading Act. This will transfer the rights and liabilities under the original contract of carriage to the new owner of the goods. This endorsement may occur any number of times. As a document of title, it can be used as a security of payment and it is a vital document among others required for a letter of credit.

Several international rules – not only, but also focused on the Bill of Lading– were proposed over the years, like the Hague Rules in 1924; an updated version was introduced in 1968 [36]. These rules were criticized for covering only transport by sea, ignoring multi-modal transports, and not recognizing the container revolution; other critics focus on the vulnerable law structure, arguing that it is greatly in favor of the vessels’ operators when compared to the shipping companies. The Hamburg Rules [37], introduced in 1978, provided a more modern approach and tackled the bias toward ship operators in the Hague-Visby rules.

The Rotterdam Rules, adopted in 2008, is a treaty that proposed new international rules, in contrast with the existing conventions. These rules also apply to multi-modal transports that involve an international sea-leg and also deal with issues not covered at the time in international law.

The Rotterdam Rules include a chapter dedicated to electronic records in view of the continuous development of systems and technologies that allow the replacement of paper documents – like the bill of lading– with electronic records. The provisions introduced aimed to regulate a possible replacement since at the time of creation there was no great success in the area [38].

The diagram in Figure 2.7 shows the typical life cycle of a modern Bill of Lading.



Source: CargoX [39]

Figure 2.7: Typical life cycle of a Bill of Lading

Types of Bills of Lading

Bills of lading can be described as negotiable or non-negotiable. Negotiable bills of lading provide clear instruction to deliver the goods to anyone in possession of the bill, which itself is a title to the goods. Non-negotiable bills of lading have a specific consignee to whom the goods are delivered, only he can claim the cargo at the destination.

Despite this, there are several types of bills of lading, some negotiable, and others non-negotiable.

Bearer Bill of Lading

A bill that states that delivery shall be made to whoever holds the bill. May be created explicitly or it is an order bill that failed to nominate the consignee whether in its original form or through a blank endorsement. This bill can be negotiated.

Order Bill of Lading

This bill uses express words to make it negotiable, this means that delivery is made to the order of the consignee using words such as “to order”. The cargo will be delivered to the bonafide holder of the bill of lading. As it is made “to order” of the consignee, it is a negotiable document of title. This bill is commonly used when goods have not been paid, in this case the intended consignee is identified as a notify party, described in Section 2.3.3.

Straight Bill of Lading

The goods are consigned to a specific person and it is not negotiable. This type of bill is also known as non-negotiable, and from a bank’s perspective it is not safe. Because of this, it is mainly used in military cargo.

House Bill of Lading

A Bill of Lading created by an Ocean Transport Intermediary (OTI), for example, a freight forwarder or a non-vessel operating carrier (NVOC), that is issued to the supplier once the cargo is received. The shipper is the actual exporter of the cargo, and the consignee will be the actual importer of the cargo.

Master Bill of Lading

A master Bill of Lading is issued by the carrier, which is a ship owner or operator. The shipper is usual the NVOC or their agent of the freight forwarder. The consignee is usually the agent, NVOC, or freight forwarder in the port of discharge that assists with the transaction.

Shipped Bill of Lading

A Bill of Lading that is issued when cargo is loaded on the vessel. Sometimes referred to as "on board" bills.

Received for shipment Bill of Lading

This bill differs from a shipped Bill of Lading in not stating that the goods received have been loaded on to a vessel. It is only recorded that the goods were received for shipment.

Through Bill of Lading

It is typically used when the main carrier undertakes a portion of the carriage, for example, the sea leg, but also undertakes to arrange, as an agent, an additional leg, for example the road portion from the discharge port.

Combined transport Bill of Lading

The combined transport Bill of Lading evidences a contract between the cargo owner and the carrier, where the carrier agrees to arrange transport of the goods between two points, even if the route between the two points involves a series of stages of sea carriage or other means, such as road or rail.

Clean/Claused Bill of Lading

If the shipowner raises an objection about the condition of the cargo, they can clause the bill of lading along with the cargo condition, making it a claused Bill of Lading. Otherwise, it is a clean Bill of Lading.

Bill of lading clauses

The usual items that appear on the face of normal bills of lading are:

- Name of the shipper: the first party of the contract of carriage, that is why it should be the name of the cargo owner and not of an agent
- Name of consignee or ‘to order’ and notify party: it can be filled with the name of the consignee or the words “to order” and the name of a “Notify party” below it. This is done when a documentary credit is used to negotiate a Bill of Lading, then it is an order bill of lading.
- Ship’s name: the name of the carrying vessel. If another vessel is used in the transport of the goods, usually the one that carries out the deep sea or main leg voyage appears in this space.
- Place of receipt / Port of loading: Place of receipt will appear depending on the type of transport or bill, port of loading should always be present. With multimodal, combined transport bills or through bills, the place of receipt is also shown.
- Port of discharge: Port of discharge is always shown, and in the same way, in the case of multimodal, combined transport or through bills, place of delivery should also appear.
- When and where freight to be paid: “freight paid”, or “payable at destination” often called “collect”. The Bill of Lading is not totally a document of title until the freight is paid and the Bill of Lading is endorsed by the carrier with the words “freight paid”.
- Number of original bills of lading: only one is necessary but usually two or three exist.
- Full description of the cargo: marks, which are used to identify packages in LCL (less than container load), container numbers and container seal numbers appear here. Also, number and kinds of packages, for example, three containers and two cases. And weight and measurement; weight is crucial in the stowage of the ship; the measurement is more relevant in LCL cargo. It is important to describe the contents of a package in a way that satisfies the letter of credit but also avoiding including anything that might suggest value.
- Place and date of the issue of the Bill of Lading: in the case of a received bill, it is the date the goods were received for shipment; if it is a ‘shipped’ Bill of Lading, the date the goods were loaded
- Signed “for the carrier”: the signature must identify the carrier and if the bills are signed by an agent on its behalf. This signature converts the bill into a document of title of goods.
- Printed clauses: this is the described evidence of contract; on the reverse of the bill the terms of the contract are spelled out.

CHAPTER 3

State of the art

This chapter introduces the electronic bill of lading and related work in the area. Several solutions will be presented, how they work and underlying technologies will also be explained, like the blockchains used. Next, we make a general analysis of the electronic bill of lading and also of all the specific solutions presented.

3.1 Blockchains

3.1.1 Ethereum

Ethereum was first conceptualized in 2013 by Vitalik Buterin. In the Ethereum yellow paper [40] Dr. Gavin Wood, says Ethereum can be described as a very specialized version of a cryptographically secure, transaction-based state machine. It is an open-source platform created to enable the use of smart contracts and consequently decentralized applications with advantages inherited from the blockchain.

It distinguishes itself from the main competitor, Bitcoin, as a programmable network serving as a marketplace for several different services, such as finance, games, art, and many others, all of this can be paid in the network currency Ether (ETH).

Ethereum enables transfers of several types of tokens that represent diverse types of assets. Blockchain currencies, or cryptocurrencies, are called fungible tokens. These tokens are interchangeable, this means that tokens of this type are equal between each other, in the Ethereum network these are the most common and are called ERC-20 tokens.

Non-fungible tokens, commonly known as NFTs, on the other hand are not interchangeable, these tokens represent unique assets. They enable a whole new set of functionalities in a blockchain. NFTs can be used to represent ownership of unique items, these items can be almost anything, they are used in art, collectibles, real estate and in the context of this study documents of title. In the Ethereum blockchain they are usually built using the standard ERC-721 [41].

3.1.2 Hyperledger Fabric

[42] Hyperledger was founded by the Linux Foundation in 2015 to advance cross-industry blockchain technologies. Instead of using a single blockchain standard, it encourages a collaborative approach to developing blockchains and open development.

Hyperledger Fabric is one of the blockchains within Hyperledger, it is a private and permissioned blockchain with smart contracts. The members need to enroll through a trusted Membership Service Provider (MSP). It has a modular and versatile design, offering pluggable options, different formats for data storage, consensus mechanisms can be swapped, and different MSPs are also supported.

This architecture separates transaction processing into three phases: distributed logic process and agreement, or chaincode; transaction ordering; and transaction validation and commitment. This division grants fewer levels of trust and verification across node types, and better network scalability and performance.

The ordering service (running on orderer nodes) receives transactions containing signed and endorsed proposal responses, from one or more applications via the gateway service, and orders and packages the transactions into blocks. These are the blocks (which are also ordered) — consisting of endorsed and ordered transactions — that make up a Fabric blockchain ledger.

A Fabric blockchain network is comprised of peers (non-ordering nodes), responsible for storing and managing copies of ledgers and smart contracts; and orderers (ordering nodes), charged with ordering and packaging of transations into blocks.

A target peer, selected by the client application, executes transactions by invoking the chaincode (smart contracts), then returns the result to the client. The transaction proposal is also forwarded to the required endorsing peers (depending on the defined endorsement policies), these will also execute the transaction and return the result. If all the responses satisfy the endorsement policies, the transaction is then forwarded to the ordering service in an ordering node.

The ordering service receives transactions, and will then order and package them into blocks. Finally the ordered blocks are sent to every peer that then validates each transaction, in the correct order, and ensures the correct endorsement [43]. If all is well, each peer commits the received block to its local copy of the ledger. The transaction lifecycle can be observed in the Figure 3.1.

Network scalability and performance is increased, since only confirming instructions are sent across the network.

A group of participants have the ability to create channels that allow them to create a separate ledger of transactions. This feature allows the existence of competitors to use the same network without having every transaction known to each other.

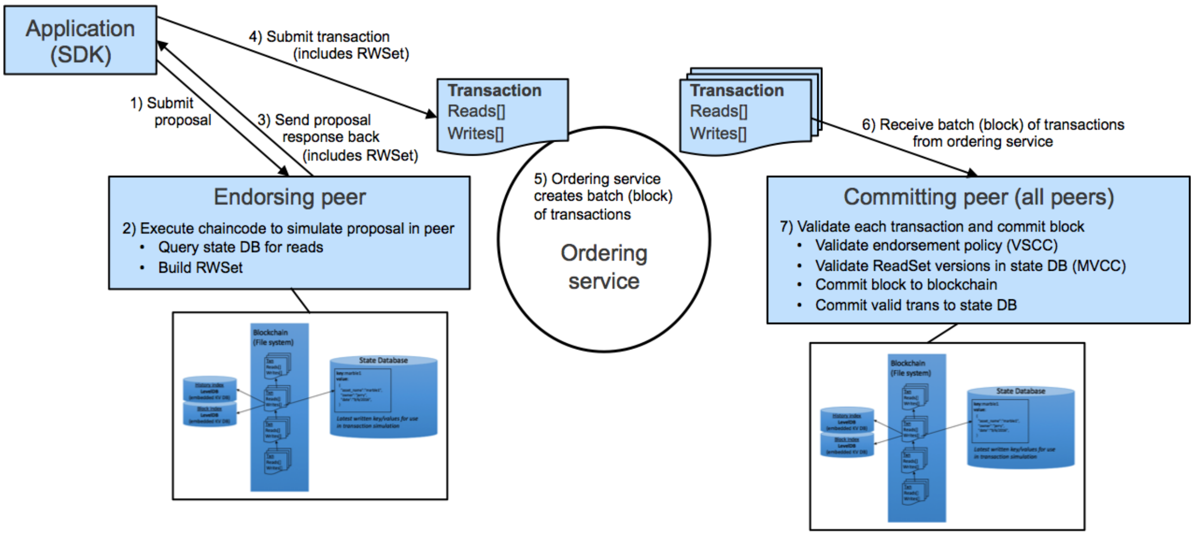

Application (SDK)
1) Submit proposal
3) Send proposal response back (includes RWSet)
4) Submit transaction (includes RWSet)
Transaction
Reads[]
Writes[]
Endorsing peer
2) Execute chaincode to simulate proposal in peer
• Query state DB for reads
• Build RWSet
5) Ordering service creates batch (block) of transactions
Ordering service
Transaction
Reads[]
Writes[]
6) Receive batch (block) of transactions from ordering service
Committing peer (all peers)
7) Validate each transaction and commit block
• Validate endorsement policy (VSCC)
• Validate ReadSet versions in state DB (MVCC)
• Commit block to blockchain
• Commit valid trans to state DB
Blockchain (File system)
State Database
Blockchain (File system)
State Database

Figure 3.1: Transaction lifecycle in Hyperledger Fabric [44]

3.1.3 Contour (Voltron)

It uses R3 Corda, another blockchain platform, as their base technology and was founded by 8 banks. Contour delivers a network for trade finance over a distributed ledger, inheriting all its benefits. Contour's initial objective was to digitally manage the issuance of letters of credit, but, even though it is still their main focus, they now also provide other electronic trade documents including documents of title like the bill of lading.

R3 Corda

Corda is not a blockchain by definition. Transactions do get cryptographically chained, however it does not have blocks to store them before confirmation, Corda confirms the transactions immediately. Corda was created as an alternative to permissionless blockchains, since it is aimed at the financial sector and banks do not want competitors to have access to their data, even encrypted. This permissioned network provides transacting parties a way to achieve a consensus without revealing sensible information, this is achieved via smart contracts.

Also, in traditional blockchains where parties are unknown, every message is broadcast to every participant. This happens because the identity of the recipient is not known and allows the network to be aware of every transaction avoiding double-spending - a phenomenon where a single unit of currency is spent simultaneously more than once. But since privacy is one of the main concerns in Corda, this solution is inadequate, all participants would see transactions from everyone else. Instead, Corda addresses each message to a specific counterparty, resulting in data being shared on a need-to-know basis only [45].

Corda reduces record-keeping and transaction costs and allows companies to streamline operations with several programs: CorDapps, Partner Connect Program, Launchpad, Venture Development, and Conclave. CorDapps (Corda Distributed Networks) are distributed applications with the goal of allowing nodes to reach agreement on updates to the ledger;

some examples are applications for public or private auctions, purchasing wellness services, managing expiry dates on food items, approving, or denying loans based on credit agency ratings, and many more. The Partner Connect Program helps new adopters to develop innovative solutions on Corda. The Launchpad, as the name suggests, is a launchpad for new CorDapps, providing developers with a space to deploy CorDapps in their early stages. Venture Development program helps startups get to market faster, offering resources and support such as workshops and access to educational content. Finally, the Conclave enables users to verify an application's integrity to guarantee sensible data security.

3.2 Electronic bill of lading - eBL

An electronic bill of lading is a paperless bill of lading electronically issued instead of a traditional printed on paper and physically issued as a hard copy.

Independent of the technology where the electronic bill of lading is issued, the bill of lading should fulfill the same functions as its traditional paper counterpart, the functions are receipt of goods, evidence of contract of carriage and document of title of goods (explained in the section 2.3.5).

Many believe the electronic bill of lading to be a game changer in the shipping industry, since it is faster, more efficient, provides cost reductions with good security and small risk. A more in-depth analysis of it is provided in Section 3.3.

The solutions presented are most of the ones approved by the International Group of Protection and Indemnity (IGP&I) clubs. The Group is organized as an unincorporated association of the 13 member Clubs and between them provide marine liability cover (protection and indemnity) for approximately 90% of the world's ocean-going tonnage [46]. Previously, the IGP&I's rules excluded liabilities in respect of the carriage of cargo under all electronic systems. In 2010 this changed when the group changed its stance and decided to cover these liabilities, but only with systems that received approval first. Approval from the IGP&I gives the same terms of indemnity coverage as paper bills of lading. Therefore, it is essential for the technologies to be approved so they can reach the global market.

3.2.1 Bolero

Bolero is the oldest and the first electronic Bill of Lading solution approved by the IGP&I. The name stands for Bill of Lading Electronic Registry Organization. It also allows other documentation like purchase orders, invoices, letters of credit, and others.

Bolero International claims that the receipt and evidence of contract functions of a bill of lading are relatively easy to achieve in an electronic world. Also, that electronic solutions are even better than traditional paper-based bills of lading when it comes to integrity of these documents given that it is correctly implemented. But the harder function to replicate would be the ability to transfer rights and obligations while maintaining the originality of the bill of lading. Therefore, an electronic bill of lading would require two components: a legal agreement and a technology that implemented the functions of the bill of lading while fulfilling the legal obligations of the agreement [47].

Based on this, the Bolero electronic Bill of Lading integrates a legal solution with a technology implementation. The parts that achieve this integration are the Bolero Rulebook [48], the Bolero Title Registry and the Bolero Messaging platform.

The Bolero Rulebook is an agreement between all the parties involved in the Bolero system, it guarantees that all users follow the same set of rules. The existence of this rulebook is justified by the lack of standard rules between countries, and its objective is to apply only the rules necessary for the electronic messaging to work. It covers maters related with the Bolero electronic Bill of Lading such as the creation of a Bolero bill of lading (Section 3.1), rights over a Bolero bill of lading (Section 3.3), transfer of possession of the Bolero bill of lading (Section 3.4); but also matters relating to the messages in the system (Section 2.2). Other rules resembling usual clauses used in bilateral agreements about electronic document communication are also present.

The Bolero Messaging platform is common for all Bolero solutions, and it is claimed that it provides two advantages over traditional databases: allows the replication of the traditional process of sending paper bills of lading supporting the sending of its electronic counterpart between parties and deliver it to the holder without the need for him to interact directly with the application.

The Bolero Title Registry is an application connected to the Bolero Messaging Platform. It records the current holder of the electronic Bill of Lading and only allows updates from him. It is a database that records the lifecycle of an electronic Bill of Lading, and ensures that it cannot be changed by anyone but the carrier and cannot be duplicated. The electronic Bill of Lading must remain unique, or original, and this is guaranteed by the title registry.

The electronic bills of lading are signed with digital certificates and the communication channels are encrypted. Bolero is audited according to auditing standard developed by the American Institute of Certified Public Accountants – SSAE16 – every year by an external auditor.

In Bolero an electronic bill of lading can only be created by a carrier or their explicit authority, it can be created directly in the app or by scanning a paper one. The document is uploaded into the system and attached to a Title Registry Instruction (TRI). The electronic Bill of Lading along with the TRI is digitally signed and sent to the first holder, usually the shipper. When it is surrendered, the carrier receives an email, and is then able to release the cargo at the discharge port.

Bolero is a cloud-based platform that can be accessed via a web interface, but also allows for integration with internal back-offices. Since it is a closed system, Bolero accepts members manually, requiring customers to register and wait for approval. This approval is only given after signing an agreement and receiving training. The system is free of charge for carriers, agents, forwarders, and operators.

Bolero is a Countour, formerly known as Voltron, contributing technology partner integrating its electronic bill of lading onto the platform [49].

3.2.2 CargoDocs by essDOCS

EssDOCS was founded in 2005, several years after Bolero. They offer a range of solutions to digitize trade finance and logistics documents, including the bill of lading via CargoDocs. At first glance CargoDocs is very similar to Bolero: both have a registry to store electronic Bills of Lading, are web-based and centralized. Besides bills of lading, essDOCS also allows the management of other documents like certificates of origin, commercial invoices, sales of goods contracts, and more. The CargoDocs solution is made of two major components, DocHub for creation & approval and DocEx for exchange & legal transfer [50].

DocHub is a document hub that allows to collaboratively create, review, and approve paper or electronic documents. DocEx (eDoc Exchange) is a solution that enables digital signing, exchange and legal transfer of title documents. Users can push documents directly from DocHub to DocEx.

EssDOCS also has an agreement that all users should sign, the Databridge Services & Users Agreement (DSUA); it regulates the operation of the solution and provides a legal framework. Only users that join this agreement can create legally effective eDocs, guaranteeing that all participants are committed to treat electronic documents as the equivalent of paper documents [51].

They are subject to annual audits focused on external penetration testing and internal vulnerability assessment and the data centers are ISO 27001 and ISO 27002 certified [52].

The creation and management of documents is similar to the traditional way. If another party is not in the system, the user can transition back to paper at any point. Supporting paper documents can be scanned, converting them into PDF's and signed, but this cannot be done with bills of lading since it is not a safe way of storing critical information.

Even though CargoDocs is a web-based solution, it also provides API's for integration in internal financial, operational or document creating systems.

EssDocs also announced a partnership with Contour in 2019 in order to integrate CargoDocs into the blockchain [53].

3.2.3 E-Title

This solution was created by ex-members of Bolero but works in a unique way than the other solutions already presented. It is a peer-to-peer network, unlike the other centralized systems. They claim that it works as well in the back-office of carriers, banks, or multinational companies as when provided by an Application Service Provider (ASP) for Small and Medium Enterprises (SMEs) [54], as shown in Figure 3.2. Like the other solutions, it also has a legal framework called Electronic Title User Agreement, written in accordance with United Nations Commission On International Trade Law (UNCITRAL) Model Law. It is aimed at filling the legislative gap by providing a private agreement between the parties that use the system, that provides a legal foundation to allow the transfer of electronic bills of lading. It was based on English common Law

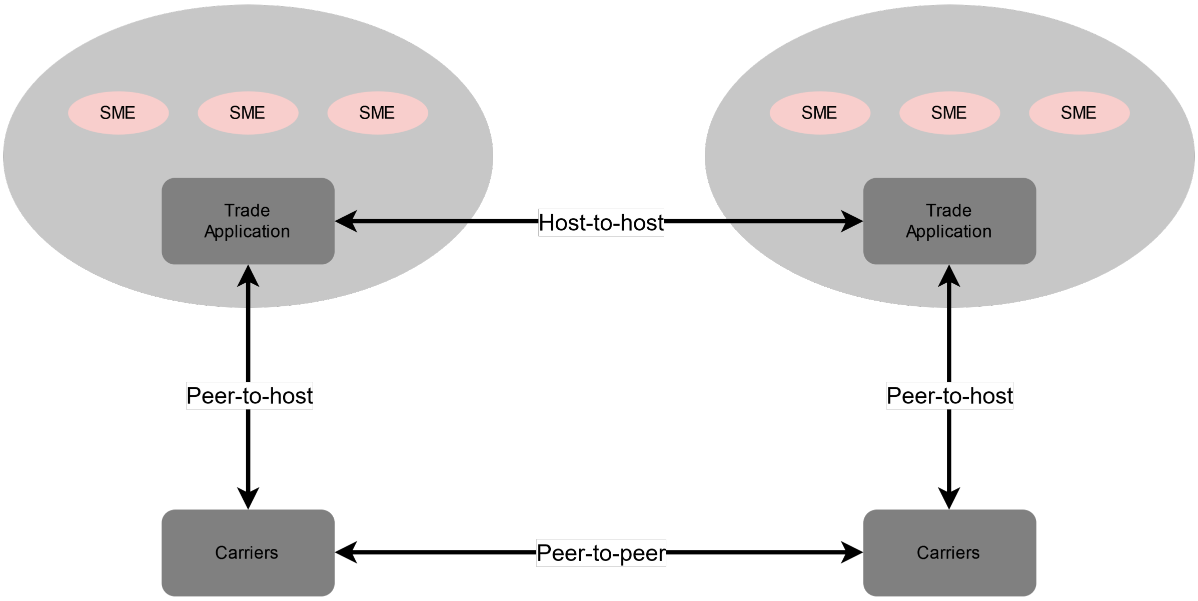


Figure 3.2: Example of ASP and SME organization on e-title

The focus of this solution is on the electronic title creation and negotiation, enabling full electronic trading, documentary credits and collections, and release of goods.

To guarantee the secure transfer of documents during negotiations, a component called Hardware Security Module (HSMs) is used. It is a tamper-proof hardware that prevents alteration and forgery of title documents, it also prevents double trading (using the same electronic title more than once).

E-Title's software is connected to companies back-office or trade documentation system. A carrier can create a bill of lading traditionally on paper or on a document creation software and send it to e-title. There, an electronic bill of lading is created, signed, and registered in the HSMs. The electronic Bill of Lading is then sent back to a carrier's back office, where it can then be redirected to the shipper. Finally, the shipper can verify the signature and that the electronic Bill of Lading remains unchanged. A more in-depth generic electronic title life cycle is shown in Figure 3.3.

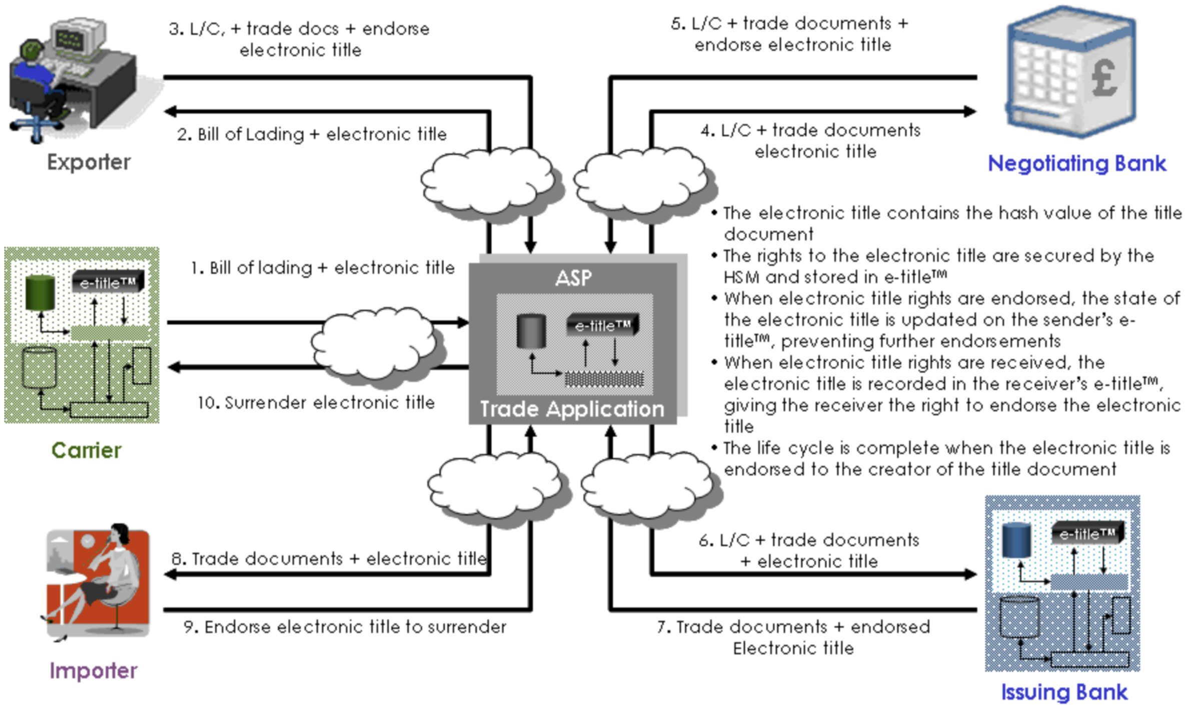

3. L/C, + trade docs + endorse electronic title
5. L/C + trade documents + endorse electronic title
2. Bill of Lading + electronic title
4. L/C + trade documents electronic title
Exporter
Negotiating Bank
• The electronic title contains the hash value of the title document
• The rights to the electronic title are secured by the HSM and stored in e-title™
• When electronic title rights are endorsed, the state of the electronic title is updated on the sender's e-title™, preventing further endorsements
• When electronic title rights are received, the electronic title is recorded in the receiver's e-title™, giving the receiver the right to endorse the electronic title
• The life cycle is complete when the electronic title is endorsed to the creator of the title document
1. Bill of lading + electronic title
e-title™
ASP
Trade Application
10. Surrender electronic title
Carrier
8. Trade documents + electronic title
6. L/C + trade documents + electronic title
9. Endorse electronic title to surrender
7. Trade documents + endorsed Electronic title
Importer
Issuing Bank

Figure 3.3: Generic in-depth electronic title lifecycle [55]

3.2.4 EdoxOnline by Global Share

The Argentinian software provider Global Share was founded in 2007 with focus on streamlining the issuance of shipping and commercial documents. EdoxOnline [56] marked the beginning of the second generation of electronic Bill of Lading systems; the key difference from the first generation is the reliance on blockchain technology. EdoxOnline's product is based on the Ethereum blockchain, and allows users to automatically issue and manage electronic Bills of Lading in collaboration with all supply chain members.

Like Bolero and essDocs, it also uses a web platform, where the instructions for a document are inserted from the destination point and sent to the exporter's country. There, exporters coordinate with other members of the supply chain who use the system to add the corresponding information. Finally, the BL can be saved as a PDF, printed, and signed.

The web platform is available to all members via a single page, but only the necessary information for each member is displayed. EdoxOnline has also integrations with other electronic Bill of Lading systems, such as Bolero and CargoDocs.

3.2.5 CargoX

CargoX is a crowdfunded project started in 2018 that counted with the contribution of thousands of individuals and companies in a KYC (Know Your Customer) procedure [57]. They claim to be one of the most market-neutral companies in logistics and want to remain independent and open to everyone.

CargoX relies on the security and decentralization provided by open blockchains and smart contracts. One of the main objectives of the company is to eliminate the need for paper documents in logistics.

Currently CargoX's solutions are built over Ethereum, since it is one of the most robust blockchains in the market, with a strong developing community, along with industry support, and a roadmap filled with innovative features for the future.

To drive the core functionalities of CargoX's smart contracts and also to serve as a payment method for logistics services, the company created the ERC-20 token CXO.

CargoX uses the Ethereum public network to transfer documents of title, such as a bill of lading. Documents uploaded to the network are stored in a distributed file system, the InterPlanetary File System, and encrypted [58]. The InterPlanetary File System (IPFS) is a protocol for storing and retrieving files from a peer-to-peer network; the files stored are content-adressable by a hash, since it uses a Merkle tree like process the Merkle Directed Acyclic Graphs (DAG), any tamper with a file will result in a change to the hash.

After being stored, the document is converted to a token, and ownership can be transferred using Ethereums public token ownership transfer capabilities. CargoX uses ERC-721 non-fungible tokens to achieve this, transactions can be signed in the decentralized application or via an API that is available for integration with back-offices.

CargoX also has a set of rules and principles that enable the platform ecosystem and logistics services to work, it is called the CargoX Document eXchange Protocol. These rules and principles are mainly enforced by the smart contracts [39].

Since the solution is built on a public blockchain, CargoX does not have the capabilities to take over ownership of any documents. Also, users can always audit the trail of title transfers and other transactions via blockchain explorers.

3.2.6 TradeLens

TradeLens is an open and neutral supply chain platform built over blockchain technology [59]. It was developed in a collaboration between GTD Solution and IBM with support from other major players in the logistics industry.

TradeLens can be divided into three main components: the ecosystem, platform, and applications and services marketplace. The ecosystem is its business network, which involves ports or terminal operators, government authorities, shippers, financial services, carriers, intermodal operators, and freight forwarders.

The platform is the digital tools provided to the entities involved, so they can share information and collaborate securely. It is achieved with a strict permissions structure based on an organization's role; this way, only the necessary parts can access information about a shipment. The logical choice of a blockchain that can implement these strict permissions is a permissioned blockchain. TradeLens uses the blockchain Hyperledger Fabric, which is a permissioned blockchain that can provide a high degree of privacy to the users.

Another focus of TradeLens is the promotion and adoption of standards and interoperability of platforms. The platform uses the Supply Chain Reference Data Model from UN/CEFACT and shares their APIs to support interoperability.

The platform is accredited with the ISO27001 security certification.

This solution addresses the broader supply chain processes and not just the shipping activity where the bill of lading is included. Exchanging the electronic Bill of Lading is a standardized process for all users and adheres to legal and regulatory frameworks. Carriers issue an electronic Bill of Lading for a shipper, the issuance is recorded, and a hash of the document is saved in the blockchain. The shipper can then view the electronic Bill of Lading on the platform, and when necessary, transfers it to the consignee. When the shipment arrives, the consignee can surrender the electronic Bill of Lading that will return to carrier for the cargo to be released.

3.3 Electronic Bill of Lading Analysis

This section starts with a SWOT analysis of the electronic bills of lading in general without specifying any of the solutions presented. Secondly, the solutions are analyzed individually according to some aspects.

3.3.1 General SWOT analysis

SWOT stands for Strengths, Weaknesses, Opportunities, and Threats. Strengths and weaknesses are related to the solutions themselves, what do they do well and what needs improvements. Opportunities and threats are external, opportunities are things that solutions can take advantage of, and threats are things that they should be protected from.

In the case of the electronic bill of lading, there are some obvious strengths. A bill of lading is usually sent three times through a courier, each time costing a certain amount of money and time. As a digital alternative to traditional paper and courier services, the issuing and transfer of the bill of lading is almost instantaneous and costs nothing. Since there are no courier fees or insurance costs, the Digital Container Shipping Association estimated a total of four billion dollars annual savings at a 50% adoption rate for the container shipping industry alone [60]. Another important strength is that it cannot be lost, damaged or destroyed during transport, an accident such as spilling a cup of coffee on the bill of lading or the courier simply losing it would cause additional costs and time delays. Also, since the transfer of a bill of lading is almost instantaneous there is never the problem of the cargo arriving before the bill of lading is in possession of the importer; if this happens, the importer will not have the required document of title to present to the carrier, potentially causing more costs to place goods in storage or losses due to market fluctuations. Finally, forgery is way more difficult in electronic bills of lading when compared to paper ones. Therefore, the strengths can be summed up in cost and time savings, more reliability and more security against accidents or intentional forgeries.

The weaknesses in electronic bills of lading are common to the ones identified by CargoX in their solution, they are not about the technology itself but more about the businesses and the industry, such as the lack of funding and marketing, electronic Bill of Lading unawareness in the shipping industry, insufficient reputation, and lack of trust in innovative technologies,

Strengths	**Weaknesses**	**Opportunities**	**Threats**
Cheaper than paper	Lack of funding	Size of the shipping industry	Adoption barriers on institutions
Almost instant issuance and transfer	Lack of marketing	Optimize supply chains	Slow adapting industry
Cannot be lost, damaged or destroyed	eBL market unwareness	Cost reductions	Poor computer literacy
Harder to forge	Insufficient reputation	Faster transfers	Lack of legislation
Higher reliability	Lack of trust in new technologies and suppliers	COVID-19	No worldwide standard
		Environmental activism	
		Possible integrations with other industries and solutions	

Table 3.1: SWOT analysis of an electronic bill of lading

like blockchains and their suppliers. Most of these weaknesses will disappear as time goes on and existing solutions prove themselves in the industry by showing their strengths.

Several factors can be a great opportunity for different electronic bill of lading solutions. The size of the shipping industry and the possible revenue that comes from it, potential to optimize supply chains, and integration with major logistics companies. Further technology development will allow even more cost reductions and faster speeds of transfer. Governments and other entities pushing for adoption of paperless trading systems due to COVID-19. The increasing awareness of environmental issues and increased pressure from the general public to adopt eco-friendly and sustainable solutions. And finally, possible integration with banking, insurance, and other institutions.

Some existing threats to the electronic Bill of Lading are institutional adoption barriers, the characteristically slow changing or developing environment of the logistics industry, poor computer literacy among users. Lack of legislation, even though a lot has been done in this area in the past decades, and slow response to international initiatives in this aspect, such as the Modern Law on Electronic Transferable Records (MLETR) formulated by UNCITRAL in 2017 [61], from governments resulting in an unclear legal status of electronic bills of lading. Lack of common standards and interoperability issues, result in slow adoption of electronic Bills of Lading, this can be seen as an opportunity for new convenient approaches and technologies but possible integrations with different entities in different industries becomes harder; Digital Container Shipping Association (DCSA), a consortium of some of the largest carriers has already published standards to facilitate acceptance and adoption, but only time will tell if this initiative is successful.

A summary of this analysis is available in Table 3.1.

3.3.2 Individual analysis

The objective of this section is to evaluate the different electronic bill of lading solutions already introduced in this study focusing on several factors and specifying each solution's unique strengths and weaknesses.

Centralization

The first electronic Bill of Lading solutions – Bolero, CargoDocs, and e-Title – which were initially centralized, did not have much success, justifying the limited acceptance and adoption in the beginning of the century. One of the main reasons for the lack of success was the centralization aspect. In a centralized system, a single entity is responsible for the traffic and operating rules in the network. This means that this entity also has access to all business transactions from every user and can even change the rules. Even though the providers of these centralized solutions have good security and privacy measures, this centralization still requires full trust in the service provider, something that some traders do not have. As a contrast, decentralized solutions, especially blockchain-based solutions, enable parties to engage in trade issuing, exchanging, and signing the bill of lading and possibly other documents without needing a central authority. These platforms simply enable the trade to occur securely and efficiently.

Privacy

When it comes to privacy in centralized solutions, it is guaranteed as long as the central authority of the system is trusted to implement security measures, such as encryption of the communication channels from the user to the central server or registry. There is still the risk of attacks on the servers that might release sensitive user information.

On blockchains the risk of attacks is decreased substantially and the technologies behind them are well-known and documented and have been proved and continue to prove to be secure. But, this does not mean that privacy is guaranteed, as explained in the Blockchain section, in a blockchain every user has a public address and any transaction made by them is associated with that public address. Therefore, if anyone knows the public address of a company, they can associate every transaction made by that public address to the company. This problem exists in solutions that use public blockchains, CargoX and edoxOnline, which are built on the Ethereum network. This can be attenuated by using private blockchains, where the members are well-known. In the case of Hyperledger Fabric used by TradeLens, this solution even supports the creation of "channels" – explained in Hyperledger Fabric subsection – that allows segregation of groups of organizations that trust each other.

Scalability

With the need to save and maintain growing amounts of data, scalability plays a big part in solutions that involve thousands and even reaching millions of active users. Scalability

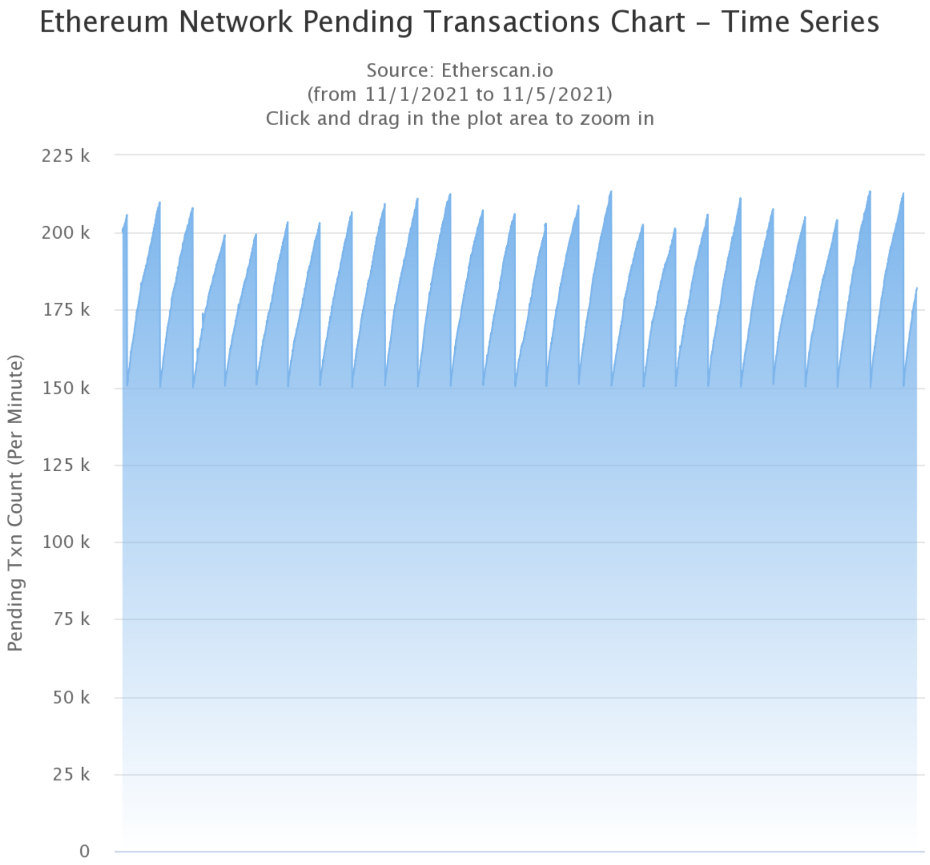


Figure 3.4: Ethereum pending transactions

is the capacity of a solution to maintain a correct functioning and good user experience even if it changes in size, typically to a larger size. Centralized solutions such as Bolero and CargoDocs may or may not be built with scalability, and might require continuous investment in infrastructure; customers have to trust that the solutions will evolve with the increase of users. Blockchains do not require as much care and investment when building solutions, but some public blockchains like Bitcoin and Ethereum, also have known problems, in a publication of late 2019 about solutions to scalability of blockchains [62], the authors reinforce the scalability issues on Ethereum and show the statistic of pending transactions per minute that went from 35000 to almost 75000; nowadays this number is ranging from 150000 to 200000 as can be seen in figure 3.4.

The scalability problems of Ethereum naturally impact the decentralized apps built over it, such as CargoX. To tackle this issue, CargoX uses a layer 2 solution called Polygon to increase speed and reduce costs that come from the increase in fees due to scalability issues. Layer 2 solutions help applications to scale up by handling transactions off the Ethereum main network (Mainnet or layer 1) [63]. Polygon has a proof-of-stake commit chain – a network that operates adjacent to the main blockchain, similar to a sidechain – where transactions are bundled and confirmed together before returning them to the main chain [64].

Hyperledger Fabric has better scalability due to the capability to organize the blockchain in separate channel that can be seen as independent networks.

Flexibility and integration

When talking about flexibility, the first that comes to mind is the TradeLens solution, built on Hyperledger Fabric, since it was built with modularity and versatility as a major priority, it can be changed to adapt to any needs that might arise. These characteristics allow Hyperledger Fabric to be used in a wide range of use cases; that is the main reason why TradeLens can be more than just an electronic bill of lading system, covering whole supply chains.

All solutions provide a web platform except for e-Title that requires software to be integrated in companies' back-offices. Solutions that provide the web platform also have APIs, allowing back office integration.

Environmentally friendly

All the solutions presented obviously have hardware and necessary amount of power to keep the systems working properly. When it comes to blockchains the consensus mechanism proof-of-work is the main point of talk on eco-friendliness. Ethereum estimated energy consumption per year in november 2021 is 83 Twh [65] (Portugal's energy consumption in 2019 was 51 Twh [66]). Furthermore, Raynor de Best estimated that a single Ethereum transaction consumes more power (178.89 kwh) than 100 000 transactions (148.63 kwh) in the VISA global payment network [67]. With these statistics, it is safe to say that Ethereum is far from being energy efficient. Applications built on Ethereum, such as CargoX and edoxOnline, are obviously responsible for some of this consumption (impossible to say how much), but they also leverage from the network's consensus mechanism. Once Ethereum completes the transition to proof-of-stake this energy consumption should reduce drastically. Carl Beekhuizen estimated on May 2021 that the proof-of-stake alternative is around 2000 times more energy efficient, resulting on a reduction in energy consumption of 99.95% [68].

A chart of Ethereum estimated energy consumption in the last years is shown in Figure 3.5.

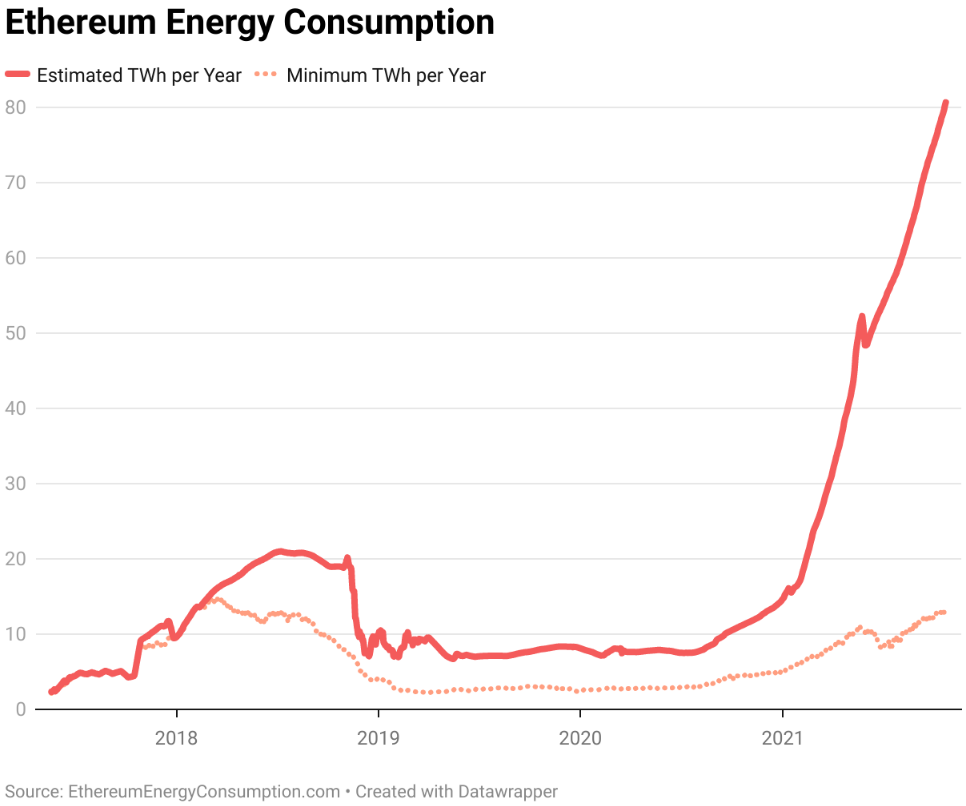


Figure 3.5: Ethereum estimated energy consumption

Individual Strengths and Weaknesses

From these and other factors it is possible to extract some strengths and weaknesses of each of the solutions. Bolero and CargoDocs (initially centralized solutions), main weakness was lack of trust, since they were centralized solutions with no proven use in the real world. The partnership with Contour may solve these weaknesses and add strengths, mainly the connectivity with the banking industry, since Contour was built with the financial system in mind. Also cross-platform connectivity with other solutions also in Contour becomes easier. CargoX and edoxOnline share advantages and weaknesses since they are both built on Ethereum and adopt some of the advantages and weaknesses. To name a few advantages, enhanced security, trust, reliability, transparency and traceability; weaknesses are low scalability, environmental unfriendliness and possible privacy problems. CargoX distincts itself from edoxOnline with the layer 2 solution Polygon, increasing efficiency and scalability greatly. Tradelens, as a solution that uses a private blockchain, will also inherit some of its characteristcs. It is a partially decentralized solution with strenghts like better performance and efficiency, along with the security and reliability provided by blockchains in general. Another major strength of this solution is its flexibility, that allows for many use cases in supply chains, not being limited to electronic Bills of Lading.

Bibliography

[1] W. Diffie and M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. DOI: 10.1109/TIT.1976.1055638.

[2] C. Paar and J. Pelzl, *Understanding Cryptography.* 2010.

[3] C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communications in a public world.* Prentice Hall of India, 2008.

[4] *The blockchain never sleeps*, https://www.crs4.it/focus-view/the-blockchain-never-sleeps/, Last accessed: 2021-11-4.

[5] H. C. A. v. Tilborg, *Encyclopedia of cryptography and security.* Springer, 2011.

[6] P. Barreto and V. Rijmen, “The whirlpool hashing function,” vol. 24, Jan. 2003.

[7] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Last accessed: 2021-11-8. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[8] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1991. DOI: 10.1007/bf00196791.

[9] L. Lamport, R. Shostak, and M. Pease, *The byzantine generals problem*, Last accessed: 2021-11-8, Oct. 2018. [Online]. Available: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf.

[10] M. Castro and B. Liskov, “Practical byzantine fault tolerance,” Last Accessed: 2021-11-8. [Online]. Available: https://pmg.csail.mit.edu/papers/osdi99.pdf.

[11] I. Bashir, *Mastering blockchain: distributed ledger technology, decentralization, and smart contracts expained.* Packt, 2018.

[12] *What is decentralization in blockchain?* Last Accessed: 2021-11-8. [Online]. Available: https://aws.amazon.com/blockchain/decentralization-in-blockchain/.

[13] T. Jung, *How transparency through blockchain helps the cybersecurity community*, Last accessed: 2021-11-8, Apr. 2019. [Online]. Available: https://www.ibm.com/blogs/blockchain/2019/04/how-transparency-through-blockchain-helps-the-cybersecurity-community/.

[14] *Art. 17 gdpr – right to erasure ('right to be forgotten').* [Online]. Available: https://gdpr-info.eu/art-17-gdpr/.

[15] R. C. Merkle, “A digital signature based on a conventional encryption function,” *Advances in Cryptology — CRYPTO '87 Lecture Notes in Computer Science*, pp. 369–378, 1988. DOI: 10.1007/3-540-48184-2_32.

[16] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017. DOI: 10.1109/bigdatacongress.2017.85. [Online]. Available: https://ieeexplore.ieee.org/document/8029379.

[17] N. Szabo, *Smart contracts*, Last accessed: 2021-11-8. [Online]. Available: https://web.archive.org/web/20160323035617/http://szabo.best.vwh.net/smart.contracts.html.

[18] *Proof-of-work (pow).* [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/.

[19] S. King and S. Nadal, *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake*, Last accessed: 2021-11-8, Aug. 2012. [Online]. Available: https://www.peercoin.net/whitepapers/peercoin-paper.pdf.

[20] C. Hoskinson, *Proof of stake*, Last accessed: 2021-11-8. [Online]. Available: https://why.cardano.org/en/introduction/proof-of-stake/.

[21] *Proof-of-stake (pos)*, Last accessed: 2021-11-8. [Online]. Available: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[22] *Core concepts*, Last accessed: 2021-11-8. [Online]. Available: https://developers.eos.io/welcome/v2.1/introduction-to-eosio/core_concepts.

[23] *Dpos*, Last accessed: 2021-11-8. [Online]. Available: https://tronprotocol.github.io/documentation-en/introduction/dpos/.

[24] *Kovan-testnet/proposal*, Last accessed: 2021-11-8. [Online]. Available: https://github.com/kovan-testnet/proposal.

[25] *Proof of authority*, Last accessed: 2021-11-8. [Online]. Available: https://docs.vechain.org/thor/learn/proof-of-authority.html.

[26] *Harvesting and poi*, Last accessed: 2021-11-8. [Online]. Available: https://nemplatform.com/harvesting-and-poi/.

[27] L. Seeley, *Introduction to sawtooth pbft*, Last accessed: 2021-11-8, Feb. 2019. [Online]. Available: https://www.hyperledger.org/blog/2019/02/13/introduction-to-sawtooth-pbft.

[28] *Proof-of-storage*, Last accessed: 2021-11-8. [Online]. Available: https://spec.filecoin.io/algorithms/pos/.

[29] *What is proof of space and time?* [Online]. Available: https://www.chia.net/faq/#faq-3.

[30] *Poc+*, Last accessed: 2021-11-8. [Online]. Available: https://www.signum.network/pocplus.html.

[31] T. Kuhrt and R. Jones, *Hyperledger sawtooth*, Last accessed: 2021-11-8, Jun. 2021. [Online]. Available: https://wiki.hyperledger.org/display/sawtooth.

[32] *Bill of exchange definition*, Last accessed: 2021-11-8, Sep. 2021. [Online]. Available: https://www.accountingtools.com/articles/what-is-a-bill-of-exchange.html.

[33] *Types of documentary credit – a comprehensive guide*, Last accessed: 2021-11-8, Nov. 2019. [Online]. Available: https://icc.academy/types-of-documentary-credit-a-comprehensive-guide-2019/.

[34] *Ucp 600*, Last accessed: 2021-11-8, 2007. [Online]. Available: http://static.elmercurio.cl/Documentos/Campo/2011/09/06/2011090611422.pdf.

[35] C. B. Mclaughlin, "The evolution of the ocean bill of lading," *The Yale Law Journal*, vol. 35, no. 5, p. 548, 1926. DOI: 10.2307/788960.

[36] *Protocol (sdr protocol) amending the international convention for the unification of certain rules of law relating to bills of lading of 25 august 1924 (the hague rules), as amended by the protocol of 23 february 1968 (visby rules)*, Last accessed: 2021-11-8, Dec. 1979. [Online]. Available: http://www.admiraltylawguide.com/conven/sdrprotocol1979.html.

[37] *United nations convention on the carriage of goods by sea (the hamburg rules)*, Last accessed: 2021-11-8, Mar. 1978. [Online]. Available: https://www.jus.uio.no/lm/un.sea.carriage.hamburg.rules.1978/.

[38] *A comparative analysis of the hague-vibsy rules, the hamburg rules and the rotterdam rules*, Last accessed: 2021-11-8, Nov. 2009. [Online]. Available: https://comitemaritime.org/wp-content/uploads/2018/05/Comparative-analysis-of-the-Hague-Visby-Rules-the-Hamburg-Rules-and-the-Rotterdam-Rules-1.pdf.

[39] *Cargox bluepaper 2021*, Last accessed: 2021-11-8, Sep. 2021. [Online]. Available: https://cargox.io/static/files/CargoX-Bluepaper-September-2021.pdf.

[40] *Ethereum: A secure decentralised generealised transaction ledger*, Last accessed: 2021-11-8. [Online]. Available: `https://ethereum.github.io/yellowpaper/paper.pdf`.

[41] *Non-fungible tokens (nft)*, Last accessed: 2021-11-8. [Online]. Available: `https://ethereum.org/en/nft/`.

[42] *Introduction*, Last accessed: 2022-1-6. [Online]. Available: `https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html`.

[43] *Peers*, Last accessed: 2022-1-6. [Online]. Available: `https://hyperledger-fabric.readthedocs.io/en/latest/peers/peers.html`.

[44] S. Cocco and G. Singh, *Top 6 technical advantages of hyperledger fabric for blockchain networks*, `https://developer.ibm.com/articles/top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/`, Last accessed: 2021-11-5, Mar. 2018.

[45] *Trade-offs*, Last accessed: 2021-11-8. [Online]. Available: `https://docs.r3.com/en/platform/corda/4.7/open-source/key-concepts-tradeoffs.html`.

[46] *About the international group*, Last accessed: 2021-11-8. [Online]. Available: `https://www.igpandi.org/about`.

[47] *Bolero insights: Electronic bill of lading for carriers, frequently asked questions*. [Online]. Available: `http://www.bolero.net/wp-content/uploads/2020/04/Bolero-Insights-Electronic-Bills-of-Lading-FAQs-NW.pdf`.

[48] *Bolero rulebook*, Last accessed: 2021-11-8. [Online]. Available: `http://www.bolero.net/wp-content/uploads/2020/04/Bolero-Insights-The-Bolero-Rulebook-NW.pdf`.

[49] *Our partners*, Last accessed: 2021-11-8. [Online]. Available: `https://www.bolero.net/partners/`.

[50] *Cargodocs overview*, Last accessed: 2021-11-8. [Online]. Available: `https://www.essdocs.com/solutions/cargodocs`.

[51] *Users agreement (dsua)*, Last accessed: 2021-11-8. [Online]. Available: `https://www.essdocs.com/capabilities/users-agreement-dsua`.

[52] *Essdocs security features*, Last accessed: 2021-11-8. [Online]. Available: `https://www.essdocs.com/resources/security`.

[53] *Essdocs enables first fully integrated paperless trade in iron ore*, Last accessed: 2021-11-8, Aug. 2019. [Online]. Available: `https://www.essdocs.com/blog/essdocs-enables-first-fully-integrated-paperless-trade-iron-ore`.

[54] *What is e-title?* Last accessed: 2021-11-8. [Online]. Available: `https://www.e-title.net/sol_what.php`.

[55] *How does e-title work?* `https://www.e-title.net/sol_work.php`, Last accessed: 2021-11-5.

[56] *Edoxonline*, Last accessed: 2021-11-8. [Online]. Available: `https://web.edoxonline.com/`.

[57] *Business overview and technology bluepaper v1.0*, Last accessed: 2021-11-8, 2018. [Online]. Available: `https://cargox.info/files/CargoX-Business-Overview-Technology-Bluepaper.pdf`.

[58] P. Vlacic and B. Cekrlic, *The legality of an electronic bill of lading*, Last accessed: 2021-11-8, Nov. 2020. [Online]. Available: `https://cargox.io/blog/legality-electronic-bill-lading/`.

[59] *Solution brief edition 3*, Last accessed: 2021-11-8. [Online]. Available: `https://s3.us.cloud-object-storage.appdomain.cloud/tradelens-web-assets/Tradelens_Solution_Brief_v3.pdf`.

[60] *Dcsa takes on ebl standardisation, calls for collaboration*, Last accessed: 2021-11-8. [Online]. Available: `https://dcsa.org/wp-content/uploads/2020/05/20200519-DCSA-taking-on-eBL.pdf`.

[61] *Uncitral model law on electronic transferable records (2017)*, Last accessed: 2021-11-8. [Online]. Available: `https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records`.

[62] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020. DOI: `10.1109/ACCESS.2020.2967218`.

[63] *Layer 2 rollups*, Last accessed: 2021-11-8, Oct. 2021. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/.

[64] *New to polygon?* Last accessed: 2021-11-8, Aug. 2021. [Online]. Available: https://docs.polygon.technology/docs/home/new-to-polygon/.

[65] *Ethereum energy consumption index*, Last accessed: 2021-11-8. [Online]. Available: https://digiconomist.net/ethereum-energy-consumption/.

[66] *Portugal*, Last accessed: 2021-11-8. [Online]. Available: https://www.iea.org/countries/portugal.

[67] *Ethereum average energy consumption per transaction compared to that of visa*, Last accessed: 2021-11-8. [Online]. Available: https://www.statista.com/statistics/1265891/ethereum-energy-consumption-transaction-comparison-visa/#statisticContainer.

[68] C. Beekhuizen, *A country's worth of power, no more!* Last accessed: 2021-11-8, May 2021. [Online]. Available: https://blog.ethereum.org/2021/05/18/country-power-no-more/.