POLITECNICO DI TORINO

Corso di Laurea Magistrale in Management and Engineering

Anno Accademico 2022-2023

Tesi di Laurea Magistrale

Blockchain and its applications: warehouse tokenization as an alternative to traditional financing

Relatore:

Prof. Bazzanella Danilo

Candidato:

Nalli Elia Vincenzo

INDEX

1. ABSTRACT

Blockchain technology has taken the stage as one of the most innovative and most versatile technologies. It's often talked about purely for speculative reasons, but the underlying technology is both simple and complex at the same time and could find many fields of application in the coming years. In this thesis there will be an overview on how Blockchain technology works, its diffusion and what applications it could have, going deep into one specific use-case.

Blockchain was born on January 3rd, 2009 with Bitcoin that was created by Satoshi Nakamoto, whose identity is unknown to this day. It is not even known if it was one person or a collective of people. From Bitcoin we came a long way and nowadays blockchain technology is catching the attention of the most disparate industrial sectors: from the health sector to banking, from art to logistics.

The specific application that will be reviewed and analyzed is warehouse tokenization as an alternative to traditional debt financing. Parmigiano Reggiano producers will be the analyzed set of potential users of this application, and the new financial instrument will be closely linked to the value of aging Parmigiano Reggiano wheels locked in the producers' warehouse, so that investors are "involved" in the cheese aging process.

2. Distributed Ledger Technology - DLT

First of all, Blockchain technology is classified as a DLT, which stands for Distributed Ledger Technology.

Let's now break down the meaning of this name, which is often misused and erroneously substituted with the term Blockchain. To be clear and precise, a Blockchain is a type of DLT, but a DLT isn't necessarily a Blockchain (i.e. by using the term DLT we could be referring to an hashgraph or a DCA-Direct Acyclic Graph). But what does DLT actually mean?

2.1. Ledger

A ledger, taking the definiton from the dictionary, is *"a book or other collection of financial accounts"*. Ledgers are the way for businesses or institutions to record credit or debit accounts, which are then used to redact financial statements. So a ledger is a record of accounts and transactions. [1][2]

As a stand-alone technology, a ledger is not innovative at all, considering it was already used in its simplest form in the Mesopotamian civilization back in 3000 B.C., where clay tablets were used to keep a written register of the amount of a certain good. Later, in the 15th century, Luca Pacioli, who is regarded as the father of accounting, created the first ever documented ledger: he used double-entry accounts. In the picture (Figure 1) there is an example of the Cash double entry account. In this specific case, we see that the cash account has increased by 400.000 + 20.000 and decreased by 1.000 + 15.000 + 800 + 1.000, resulting in a total Cash balance of 402.200.

Cash A/C ($)

Jan 01	400,000	Jan 02	1000
Jan 29	20,000	Jan 03	15,000
		Jan 07	800
		Jan 30	1,000
Jan 30	402,200		

Figure 1. Sample double entry account.

By gathering all of these accounts in a single document we obtain what is called master ledger or general ledger, which is nothing more than a record of all the accounts and respective transactions

of a company or financial entity. In the picture below (Figure 2) there's an example of a ledger, where the Cash account from above is recorded together with all the other accounts pertinent to that financial entity. [3]

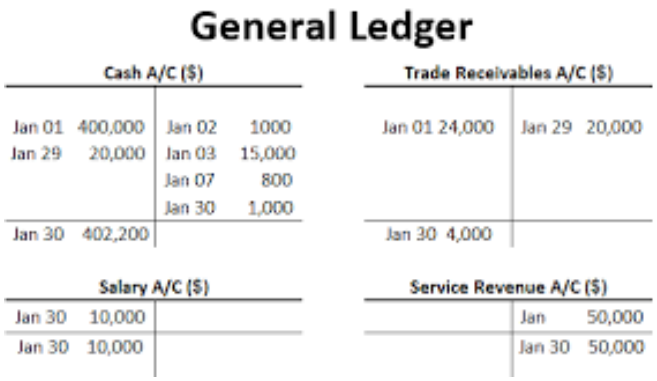

Figure 2. General ledger sample

Up to the advent of this new technology, ledgers were a mere tool for a single entity or institution to keep all their accounts updated and to redact financial statements when necessary. As we'll see along this discussion, DLTs overturned this.

2.2. Distributed

Distributed, always taking the definition from the dictionary, means *"shared or spread out"*. In this case, "spread out", is from a geographical point of view. This means that in a distributed system (ledger in this case) all actors (nodes), that are located in different parts of the globe, have access to the same data, have the same weight in the system and there is no centralized failure point, since the failure of one actor (or node) wouldn't compromise the integrity of the whole system. This is opposed to a centralized system where the whole network depends on a single node, which may lead to centralized failure, meaning that the failure of the central node would mean the failure of the whole system. As an example, a bank is a centralized system, where if the bank fails, meaning that it either gets hacked or decides to withdraw all the funds, all the users will be impacted, and can't do anything about it. If instead the bank was a distributed entity, if one actor of the bank wanted to hack the system, it would just be excluded from the entity and the users' funds would be safe.

Centralized systems heavily rely on trust, whereas decentralized systems are said to be trustless, so there is no trust issue between nodes and users, since all the rules are programmed and embedded in each DLT's protocol (set of rules).

Between centralized and distributed, there is "decentralized" ,which stands for a system where there is not a single centralized decision point (or node), but there are multiple decision nodes that share the "burden" of decision taking that communicate with each other.

For this reason a decentralized system is a subset of a distributed system, where there are various "decision" nodes (decentralized trait), all with the same importance, that are located in different parts of the world, so they potentially don't even know each other (distributed trait).

The duty of the nodes, that are those that communicate with each other during the decision making process, is to make sure that data within the DLT always stays coherent and consistent over time. [4]

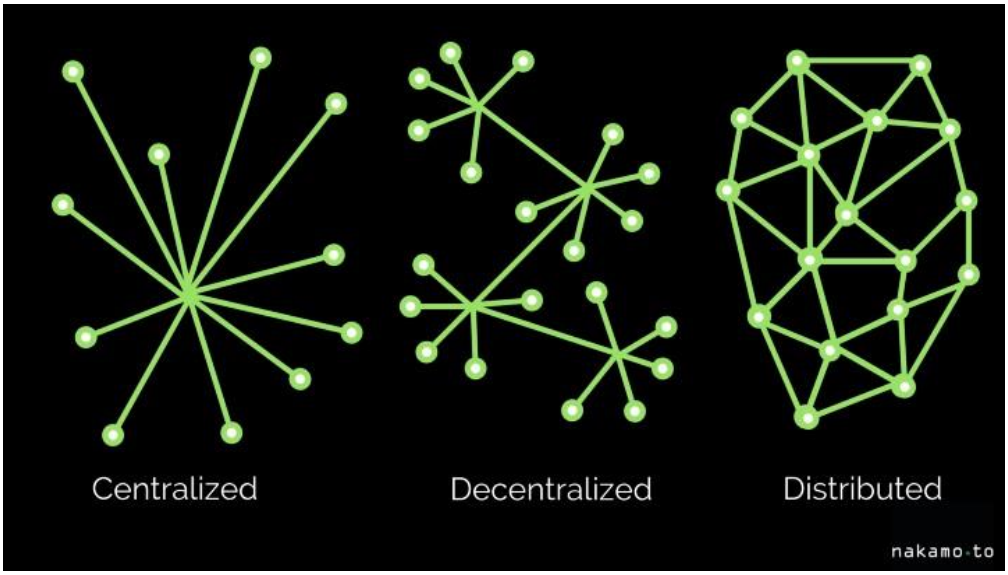

Figure 3 Visual representation of a Centralized, Decentralized and Distributed network

To sum up this brief introduction to DLTs, Hedera Hashgraph's website comes in handy: "A distributed ledger is a database shared by multiple participants in which each participant maintains and updates a synchronized copy of the data. Distributed ledgers allow members to securely verify, execute, and record their own transactions without relying on an intermediary, such as a bank, broker, or auditor." [5]

So a DLT is not just a publicly accessible database that can be modified by everyone, but it's a distributed database that works, is kept consistent and functioning thanks to the participants (nodes) that actively support the ledger. To make sure such actors exist, DLTs must provide incentives to become a node.

3. Blockchain and its essential elements

Focusing the spotlight on blockchain technology and what it really is, it can be said that it is a kind of DLT, and consists of a distributed immutable record of hashed transactions (which means it is a ledger with transactional data written with alphanumeric strings), which are then grouped into blocks. Each block doesn't just contain transactions, but it also contains information about the previous block (to be precise it contains the previous block's hash, which can be seen as its name), making each subsequent block chained to its predecessor. To use an everyday example, it is like a family tree (with only one branch) where each person (block in this specific case) inherits genes from its predecessor (so it contains information of who came before him), and so it's possible to build an immutable record where each person inherits information about its predecessor and gives information to those coming after.

Leaving family out of this matter, let's explain how a blockchain actually works and how it can be run and maintained in a trustless way by multiple actors and not having to rely on one single central node.

To do so, more definitions and roles explanation within a blockchain are needed. As a reference, the first ever created Blockchain will be used: Bitcoin's Blockchain (from now on Bitcoin will be the blockchain and bitcoin/BTC will be the related digital asset). The first line of Bitcoin's White Paper states that Bitcoin was born for the purpose of creating "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution".

Basically, Bitcoin was born in order to cancel the trust element from transactions, and create a trustless payment system. In the first block ever created on this blockchain, there were included the words "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" as a protest against the traditional monetary system.

Bitcoin's blockchain will be used to explain what a blockchain is usually made up of, but it should be kept in consideration that the names and roles can change among different blockchains, although the logic and functioning is more or less similar for all blockchains.

3.1. Block

Blocks are the fundamental element of a blockchain and each of them contains transactions and other information. A Bitcoin block is made up by [6]:

- Block size in Bytes
- Block's hash
- Block header
- Transaction counter
- Transactions

The block header then contains three sets of metadata in it:

1.
    a. Version, keeps track of protocol versions/updates. Currently, Bitcoin is in its 24.0.1 version
    b. Previous block's hash, which is the element that chains together all the blocks
2.
    a. Difficulty, set by the Proof of Work consensus algorithm
    b. Timestamp of when the block was added to the chain
    c. Nonce, value that makes sure that the block's hash respects the difficulty
3.
    a. Merkle tree root that is a summary of all the transactions of the block

In Table 1, it's possible to observe the structure of a block:

Block height: 301298
Block size: 64,842 bytes
Block hash: 00000000000000005f7803b7a502bd584177b31bfc82728cdbf4fb175cd5ae55
HEADER
Version: 0x02
Hash Previous Block: 00000000000000031d20e6ec12f70ec3ec921cda8df8a8110ddfc0d3bd0478e
Timestamp: 2014-05-18 03:24:06 GMT +2
Bits: 410,792,019
Difficulty: 8,853,416,309.13
Nonce: 3,158,001,959
Hash Merkle Root: 624465682eb7034453bc429c2cfb1db6187404d1956de10d8e750328aa813b69
Number of transactions: 128
Block reward: 25.01864355 BTC
Transactions:
Transaction 1 Hash: 7de33938e9b7495db38d3a51aefc04e4ab21808bc3b1d0475c20a86e4858998c
Transaction 2 Hash: a6d6e434b80eb9d1098e93c0a5ae1dfbec983f4e876e3106ad8f6a14e81abc27
Transaction n Hash: ……

Table 1. Block's structure

3.2. Consensus algorithm

The consensus algorithm is the mechanism through which it is ensured that all nodes reach an agreement (so reach consensus) on the state of the network at each instant in time. In Bitcoin's case, this algorithm is called Proof of Work, that as the name suggests, is based on the nodes doing some kind of work and subsequently giving proof of it to all other nodes that will check if the work was done correctly.

The work Proof of Work nodes have to do is to find a value, called nonce, that respects the difficulty condition imposed by the blockchain's protocol (set of rules). The work done to find this nonce is computational effort, so those that will want to participate in the PoW consensus algorithm, will have to invest funds in hardware and energy to make the hardware run and put all of this to the blockchain's service.

Once the nonce is found, the node that found it will communicate the nonce and the block to all the other nodes that will check whether the solution is correct: if it is, the block is successfully added to the blockchain.

Proof of Work (PoW) was the first consensus algorithm, but is not the only one. Later, another type of consensus algorithm was developed: Proof of Stake (PoS), which is nowadays used by some of the most important blockchains like Ethereum, Polkadot, Cosmos and many others. In PoS, those that want to become nodes of a blockchain, need to stake and lock the tokens of that specific blockchain as a insurance that they will behave correctly and won't behave maliciously, otherwise they will lose factions or the whole staked amount (for example, to become a node on Ethereum you must stake 32 ETH which is worth as of February 2nd 2023 around $ 51.000). Once a block is formed by putting together a group of transactions, the system randomly selects a node (validator) among the stakers, and that node will add the block to the chain.

So PoW and PoS present some substantial differences:

- In PoW the initial capital expenditure is needed to buy the hardware and to pay the electricity to run all the equipment that will be used for the computational work, in PoS the initial expenditure is the acquisition of the crypto currency that needs to be staked in order to become a validator. It is still debated which one of the two consensus algorithms is the one that leads to the most decentralization.

- In PoW there is competition among nodes, since each one of them wants to be most powerful, increasing its chances of being the node that finds the nonce and that receives the reward for doing so. In PoS, there is no such competitive dynamics, the reward is a % of the amount staked, so the higher the amount staked, the higher the rewards.
- PoW uses electricity as a resource, so it is not very environmentally friendly. PoS on the other side consumes 99.9% less electricity than PoW.

3.3. Actors of Bitcoin

The actors that need to reach consensus about the blockchain's state are called nodes and in Bitcoin we can find different kinds of nodes. The main ones are:

- Full nodes
- Miner nodes or miners
- Light nodes

3.3.1. Full Nodes

These nodes store the entire up-to-date blockchain, are the transaction verifiers, can mine blocks and have a wallet function too.

When a new transaction is created, a full node verifies that the transaction is valid and coherent with the blockchain's history.

The main verifications executed are the following:

- Check that the amount of bitcoin in the transaction isn't being double spent
- Check that the format of the transaction is correct
- Check that the data is coherent with the rest of the blockchain
- Check that the transaction has been correctly signed

If the transaction respects Bitcoin's rules, then it is successfully verified. The transaction is then put in a pool of verified transactions where miners pick from to create blocks.

3.3.2. Miners

These nodes are a subset of full nodes because they just store the whole blockchain, mine the blocks and add them to the blockchain. This is where the Proof of Work comes into play: miners put together a set of transactions in a block (called candidate block, which has a maximum

dimension of 1MB, which is equal to roughly 2000 transactions per block). At that point all the miners hash (convert the information in the block into a 64 alphanumeric characters string) the whole candidate block and will have to find the nonce that, when added to the hashed information, is lower than a value (called difficulty) set by the PoW algorithm. Bitcoin's PoW algorithm makes sure that the average time to add a block is 10 minutes. This is enabled by changing the algorithm difficulty value.

The first miner to find the nonce will be entitled to add that block to the chain. It then transmits the block to all other nodes that will check if the solution is correct. If so, the block is successfully added to the blockchain and the miner will receive a payoff for its work, called reward. Rewards are the mechanisms through which additional BTC coins are added to the circulating supply: just like miners put new gold in circulation when they mine gold, Bitcoin miners add BTC to the system when they successfully add (or mine) a block to the chain. Rewards are made of a fixed part (currently set at 6.25 BTC per mined block) plus a variable part, made up by the gas or transaction fees.

3.3.3. Light Nodes

This type of node does not store the entire blockchain, but stores only the header of each block that states the validity of a block. This allows them to transact on the Bitcoin chain. Light nodes however can't verify the blockchain, so they need to connect to full nodes to get the blocks' data.

3.4. Blockchain's incentives and chain security

In order for such a decentralized organization to seamlessly work, all the actors, especially those that keep the blockchain running and protect it, must have incentives of some kind. For nodes, in particular those that mine blocks (so full nodes and miners) on Bitcoin, the incentive is formed by the so-called "reward" and the transaction fees. When a miner successfully mines a new block, meaning successfully adds a block to the blockchain, it will receive the reward, which currently sits at 6.25 BTC per block plus transaction fees, that are paid by the users to the miners whenever they send transactions. If a user decides to pay higher transaction fees, miners will decide to validate and mine the block with that transaction in it earlier than those with lower transaction fees.

The amount of the reward was decided when Bitcoin's protocol was designed: the reward started off at 50 BTC in January 2009, and by design, the reward is halved after 210.000 blocks, which

occurs roughly around every 4 years. The reward was then halved to 25 BTC in November 2012, 12.5 BTC in July 2016 and the last halving to 6.25 was in May 2020.

Reward dynamics were designed by Satoshi Nakamoto to simulate precious materials extraction (or mining): at first it's easy and the payoff is very high (few miners competing and high rewards), as time passes, the more is mined, the higher the effort (high competition among more miners) to extract a lower amount (halved reward) than the beginning. As the material becomes more scarce and harder to extract, the higher the value it will be given. As we see in the graph below (Figure 4), BTC price has been increasing since it was first created. As BTC price increases over time, more and more people will be willing to invest to become miners in order to receive their reward. Having more and more people involved in mining means ultimately more decentralization and safety for the chain. Miners will keep receiving rewards until the whole BTC supply is mined, which is determined by the protocol to be 2.1 million BTC. After that event, they will keep getting transaction fees from all the transactions being executed on the blockchain as payoff for adding blocks to the chain. [7]

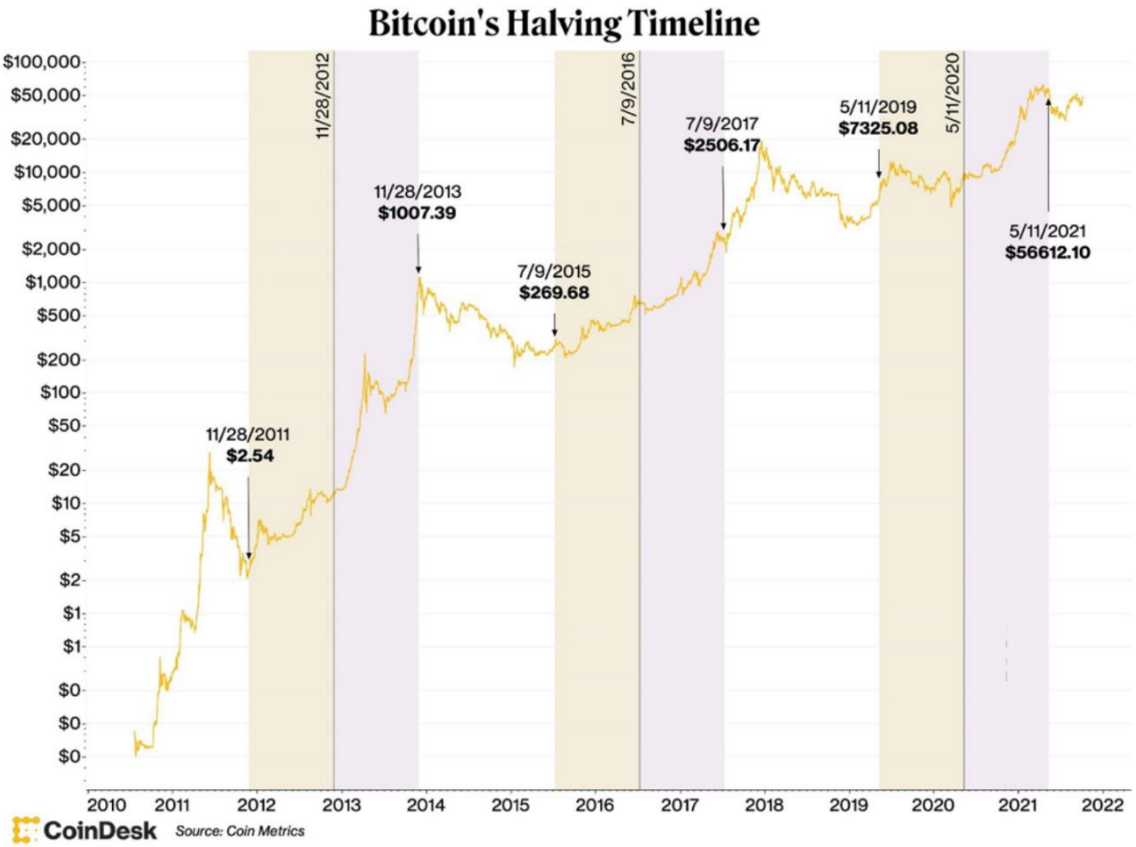

Figure 4. Bitcoin's halving Timeline

The reward is also the chain's self protection against malevolent actors on the chain: if at least 51% of the whole computing power (called hashrate) was in the hands of malevolent agents, they could possibly double spend tokens or block transactions from being approved. The more people invest in becoming miners, the more computing power will be available for the network, the harder and more costly it will be for a malevolent actor to attain 51% of the whole computing power given the high cost of the mining hardware that is required. This is called "51% attack", and blockchain developers must be able to design blockchains that can easily grown in decentralization in order to decrease the chances of such an attack.

3.4.1. Prisoners' dilemma applied to blockchain

Since the reward is both an incentive for miners and a protection, a crypto asset is fundamental for a blockchain's functioning. Every blockchain has its own native crypto asset, independently on what consensus algorithm is used: Bitcoin has BTC, Ethereum has Ether, Cosmos has Atom and so on. This protection/incentive dynamic was most likely developed by taking inspiration from Game Theory, especially the famous "prisoners' dilemma": Elia and Vincenzo have been arrested and are accomplices. The officers ask Elia and Vincenzo to confess their crimes. If they both collaborate, they both serve 1 year in prison, if one collaborates ratting (confessing) on the other and the other doesn't talk, who ratted doesn't go in jail, the other serves 5 years. If they both don't collaborate, they both get 3 years of jail time. Green highlighting shows what each individual's optimal solution is, red highlights the system's optimal solution (Table 1). [8]

The numbers indicate each prisoner's jail time if they do the action in column. The numbers' order is (Payoff Prisoner 1, Payoff Prisoner 2)		**Prisoner 2**	
		Talk	**Not talk**
Prisoner 1	**Talk**	(1,1)	(0,5)
	Not talk	(5,0)	(3,3)

Table 2. Prisoners' dilemma

So naturally, Elia would decide to rat on Vincenzo in order to optimize its own result thinking that Vincenzo will not talk, so Elia would do no jail time and Vincenzo would do 5 years. The same reasoning goes for Vincenzo, who will betray Elia thinking he will be loyal. Once they both rat on each other, they get to serve 3 years each. So in the end, it would've been better for both to collaborate, since it would've led to the optimal solution for the system (1+1 years), although it would've been a sub-optimal result for each of them (best option possible was doing 0 years in prison). This logic occurs in the same way among blockchain nodes. Let's consider two miners, miner 1 and 2. Miner 1 wants to maximize its own payoff, so will try to corrupt the system, assuming that miner 2 will behave correctly. With the same reasoning, Miner 2 wants to maximize its own payoff, so will try to cheat, assuming that miner 1 will behave correctly. At this point there can be two situations:

- If a node misbehaves and the other behaves correctly, the fraudulent node is excluding itself from adding blocks and getting any reward for its work, while the honest node will get all the payoff.

- Both nodes behave fraudulently and won't get any payoff since no block will be added to the chain and won't get any reward. Moreover, they will most likely be excluded from future possibilities of mining blocks.

Given the scenarios above, the miners are incentivized to behave according to the blockchain's protocol, which will lead both to having an individual sub-optimal payoff, that is actually the optimal payoff for the whole blockchain system. Having all nodes work correctly leads to a blockchain that works as it is intended to, creating the trustless peer-to-peer system that Satoshi Nakamoto intended to create.

3.5. Let's put everything together now: How does a transaction occur?

3.5.1. Crypto wallets

First of all, the users that are transacting on a blockchain, must first set up a crypto currency wallet, that can be seen as a password manager and store. The core functionality of a crypto wallet is to store the private key, that is the key element that allows users to keep their crypto assets safe.

So creating a wallet, generates the necessary information that allow users to send, receive or spend crypto assets.

When creating a wallet, two cryptographic keys are created:

- a public key, which can be seen as an email address: the public key is an address for a location on the blockchain where coins can be sent to. Just like an email address and as the name suggests, the public key that can be shared to anyone.
- a private key that is a long random alpha-numeric string. The private key should never be disclosed, since it's the key that allows to send crypto assets from one wallet to another. The private key is the element that certifies that the owner of that wallet has consented to the transaction. So if someone other than the owner gets the private key to that wallet, it would be able to transact from that wallet as if it was the owner. Making the private key public would be like giving the passwords of the bank account: everyone could then dispose of your funds as they prefer.

Satoshi Nakamoto also gave the definition of what a bitcoin is: "We define a bitcoin as a chain of digital signatures. Each owner transfers bitcoin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership."

This means that wallets don't "physically" contain an amount of BTC, but bitcoin can be seen as a letter that is sent from user to user, and the signatures of each user that received and sent it is recorded on the letter.

To keep track of users' funds, Bitcoin uses UTXOs.

3.5.2. UTXO - Unspent Transaction Output

Whenever someone receives an amount of BTC, that amount from the point of view of the sender is an output. So when the receiver receives those BTC, they will be recorded as unspent transaction outputs (UTXO). UTXO are not divisible, so when someone wants to send an amount X to someone else, it will have to input an amount of UTXOs greater or equal to the amount it actually desires to send. The desired amount will be then sent to the receiver and the "change" will be sent back to the sender. For instance, Elia has a total of 1.5 BTC that were received split into two transactions of 1.2 and 0.3 BTC. 1.5 is the total Unspent Transaction Output that Elia can send. Elia wants to send 1 BTC to Vincenzo, so as Inputs of this transaction he will have to pick the

1.2 BTC UTXO. He will then select the Outputs of the transactions, that will be Vincenzo's wallet as the receiver of 1 BTC in total and a "change" wallet so that Elia gets back the difference between the sum of the UTXOs sent amount minus the transaction fees. So for transactions on Bitcoin's blockchain, there will always be at least 1 Inputs and at least 2 Outputs.

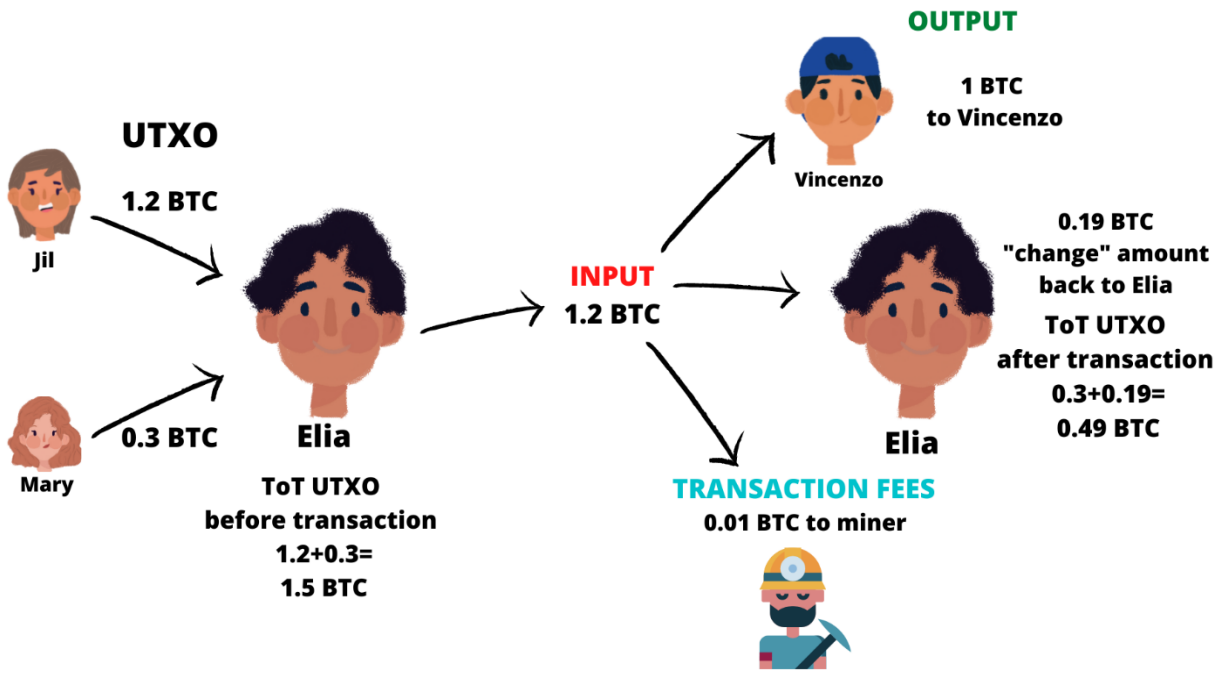

Figure 5. Bitcoin UTXO

Ethereum blockchain instead works with a balance based model that keeps track of a user's funds as a global state, so Elia in the previous case would have 1.5 ETH total and if he wanted to send 1 ETH to Vincenzo he would've just selected 1 ETH as output plus the transaction fees.

3.5.3. Sample transaction

Let's now analyze how a transaction is elaborated from a cryptographic point of view on Bitcoin's blockchain by putting together all the information provided up to now, keeping in mind that all other blockchains follow more or less the same principles and dynamics. What changes from one blockchain to another is the way nodes reach consensus. The transaction will be shown from different points of view:

- The sender (Elia)

- The receiver (Vincenzo)

- The network.

The main phases for a transaction to be added to the blockchain are:

- Elia wants to transact with Vincenzo
- Elia sends the transaction
- The transaction is validated and added to the confirmed transactions' pool
- The transaction is included in a block
- A miner is able to find the nonce and mines the block
- The block is shared with the whole network for validation
- Once this block receives enough validation, the miner receives its reward plus the transaction fees

Elia wants to send bitcoin to Vincenzo.

In order to do this, they will both need to have a crypto wallet. The keys that are generated when creating a new wallet will be used to sign the transactions and they ensure:

- Integrity: it proves that the transaction content was not corrupted by a bad actor, and allows Vincenzo to see if the transaction was corrupted
- Authenticity: allows Vincenzo (the receiver) to be sure that the transaction he received was actually sent by Elia (the sender) and not by a bad actor, who was impersonating Elia
- Non-repudiation: makes sure that Elia can't repudiate the transaction he signed

For the sake of this example, the transaction Elia sends to Vincenzo will actually be a message. The cryptographic mechanism works in the same way if the subject of the transaction were BTC. When Elia sends the transaction he will send information about the transaction (timestamp, transaction fees...) and the digital asset (message in this case). All these elements are then hashed (using SHA256 algorithm), returning a 256 bit string.

SHA256 algorithm hashes (converts) in a completely random and non-predictable way the data inserted in the algorithm, but it will always hash the same message in the same way, returning always the same 256 bit value.

Let's see a practical example on this blockchain simulator (scan QR code to access the simlator)[9]:

If the message "Hi Vincenzo!" is added as input, the algorithm will return this 256 bit string:

d9bb8d6d0f52a3021f8f6a0a1a7743c0a775b8162a79159b1dbb12eed836a392

If instead "Hi vincenzo!" is added as input (changing V from v), SHA256 will return a completely different hash:

1d2ca4be15d412d63b72dde3e0474097b0230d7dc6c4851edb221f8265a8c145

After hashing the message, Elia signs the message with his private key, which means adding the private key's alpha-numeric characters to the message. After Elia has signed the message, Vincenzo will receive three pieces of information: the plain message, that can be seen as a plain text for simplicity (made by information and the digital asset transaction), the digital signature and Elia's public key.

Vincenzo at this point will do two things:

- By using Elia's public key, will decrypt the hashed message, and will obtain the 256 bit value he hashed at the beginning, so the hash of "Hi Vincenzo!"
- Will hash the plain message ("Hi Vincenzo!") sent by Elia by using the SHA256 algorithm, that as said above, will return a 256 bit string.

Since SHA256 algorithm always hashes the same text in the same way, Vincenzo will understand whether there are some inconsistencies in what he received from Elia: the two hashed messages must be exactly the same, otherwise the information has been corrupted during the transmission. In this way all the three properties (integrity, authenticity, non-repudiation) are respected and enhanced by asymmetric encryption.

This is what a transaction looks like from the perspective of the two peers that are transacting.

Let's concentrate now on how the network and the nodes manage transactions. When Elia sends the transaction, the nodes need to verify that it respects Bitcoin's protocol (or set of rules). Once

the transaction is verified and legitimized, it is put in a pool of approved transactions, where miners pick from to create blocks to be mined.

For simplicity we will suppose that only the transaction between Elia and Vincenzo is put into a block, although usually blocks contain more than one transaction in them.

At this point, miners will start competing on who can elaborate first the block containing the transaction. The competition is on who finds first the nonce that, when added to the block's information, makes its hashed value lower than a value decided by Bitcoin's protocol, called difficulty. In order to have a higher chance of finding the correct nonce, miners invest in hardware upgrades, so they increase their computational power. Once a node is able to find the nonce that verifies the difficulty condition, that node propagates the information to all the other nodes, that will then be able verify whether the nonce is correct or not. This verification is done always by using the SHA256 algorithm to hash the block information and the nonce together. This algorithm univocally hashes the same text in the same way every time it is used, so when the nodes verify if the solution is correct, they will immediately understand if it is actually correct by hashing the block's information and the nonce. As a MasterZ course teacher once said "Proof of Work is like a Rubik's cube: difficult to solve but really easy to verify if it's correct".

To see a visual example of it, scan the QR code to access the simulator [10].

Considering "Hi Vincenzo!" as the transaction information we can see all the information contained in the block (timestamp, block number, previous block's hash, ecc) that needs to be hashed. This platform will simulate the action of a miner that has to find the nonce that respects the difficulty (which in this website's case is that the hash must start with 0000). Once the block is mined, so the nonce is successfully found, the block and the nonce are shared to the rest of the nodes which will then just input the block information and the nonce and check whether the difficulty condition is respected. In our case, we're mining block number 1, the previous hash's block is a default all zero 256 bit value and we don't have any further information, given that it is a simplified simulation of a blockchain. If we input "Hi Vincenzo!" in the data field, click Mine, we

see how the nonce that respects the difficulty rule is 9876. At this point the block is successfully added to the blockchain and all the other nodes check the correctness of the nonce and add the block to their ledger

What has been explained with this sample transaction is the Proof of Work consensus mechanism put in action, from the perspective of all the actors of Bitcoin's blockchain.

4. What came after Bitcoin?

Bitcoin is classified as a Generation 1 Blockchain: the scope of Gen1 blockchains was to create a digital currency that could work in a trustless manner, without any third party involved and to create a new financial tool. The best example of Gen 1 blockchains is Bitcoin.

4.1. Generation 2 blockchains and smart contracts

Generation 2 Blockchains later came up. The first blockchain of this type was Ethereum.

Gen2 blockchains can be seen as "programmable" blockchains, since code can be written and executed on-chain. Thanks to this evolution, a huge variety of possibilities opened, especially one interesting function: Smart Contracts. (On Ethereum) This is possible thanks to the EVM (Ethereum Virtual Machine), that allows the nodes to run code on-chain, and maintain the code in an executed state. You can think of the EVM as a big single computer composed of the network's nodes.

The concept of smart contract was initially explained by Nick Szabo in the late 90s: "A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.

Some technologies that exist today can be considered as crude smart contracts, for example POS terminals and cards."[11]

It looks like Nick Szabo already took a glimpse to the future with this definition, in which he was able to define quite narrowly what a smart contract is and its possible application fields.

So smart contracts are "self executing agreements made between two parties".[12]

They work with a "if…then…otherwise…" logic. Smart contracts opens up to many applications of blockchain: through smart contracts it is in fact possible to automate many processes that could be subject to human mistake or malignity, for example the triggering of a transaction when a certain measurable condition is reached. Together with the trustless trait of blockchain, smart

contracts could make sure that no the conditions of the agreement are always respected and correctly fulfilled.

It would be perhaps more difficult to use smart contracts for those use cases where human discretion is fundamental and central to determine whether the terms of the agreement were respected or were breached, think about the construction of a house: the house could be built and finished but not be compliant to construction rules and norms. In this case the intervention of a human being is fundamental in order to evaluate if the house is compliant. This occurs because smart contracts are fundamentally lines of code, meaning that they are not flexible and can't be bent every time there is some exception to be made.

Since blockchains are immutable, once a smart contract is deployed on a blockchain, it can't be modified, but data/information can only be appended, meaning it can be added in order to correct any flaws that are identified. This occurs because Blockchains have basically two functions: Read and Write. By writing something on a blockchain we mean doing a transaction that changes the current state of the blockchain but doesn't modify past data and information. For example I have an ETH balance of 2 ETH in my wallet, I send 1 ETH to a friend and this new transaction is written on the blockchain, my balance is changed to 1 ETH, but the fact that at one point in time I had 2 ETH balance stays stored on the chain. Following this reasoning, when a smart contract is deployed on a blockchain it stays there forever and can't be modified, but transactions can be added (writing new functions) to change its actions or to correct any mistakes. This is both an upside and a downside of blockchain: data is stored forever in the blockchain and can't be modified which gives a detailed track record of the events but this makes the burden of what is being written on the chain higher.

This opposes traditional databases that work with a CRUD logic: Create, Read, Update, Delete. This means. Create means adding a new line of information in the database, for example a new customer's name, surname, address and balance. The Read function allows to read what is written in the database. The Update function gives the possibility to change the data of the customer, for example the address. Once the update is done, there won't be a track record of what was written before. The Delete function allows to delete information from a database, which could lead to inconsistency problems in the databases and once the information is deleted, it is not retrievable anymore, which could be even a greater problem. [13]

Going back to smart contracts and why they could change the way we transact in everyday life. Think of implementing blockchain payments in a vending machine: once the selected good is correctly dispensed, crypto assets are taken from the person's account. Nowadays it's the other way around: people trust the vending machine to dispense the correct good after it's been paid for, and every time the good gets stuck or the money is just taken without dispensing the good, users would get mad with the vending machine, meaning they are disappointed of trusting the machine . A smart contract could solve this trust issue and it could work in this way:

- the user selects the good he/she wants. Let's suppose he wants a drink that costs 1 ETH. He signs the vending machine's smart contract and money is taken from his wallet and deposited in the smart contract.
- "**if** the good that the user chose is successfully dispensed, **then** the money is transferred from the smart contract to the vending machine, **otherwise** the money is given back to the user"

To make it even more fair and trustless, the vending machine could put in the contract the same amount (or half or any amount that aligns incentives for both actor to behave correctly), so that if the product isn't dispensed, the user gets his money back and gets more from the vending company as a compensation for the disservice. This would make sure that the users can don't have to trust neither the vending machine nor the smart contract, since making a faulty machine would lead to losing money, and making a breachable smart contract would lead to the vending machine company to lose the money that is in that moment stored in the smart contract.

4.1.1. Tokens

With the introduction of smart contracts, another fundamental element to Gen2 blockchains was introduced: tokens.

Tokens are secondary digital assets, opposed to the native digital assets of a blockchain, that are the assets miners receive as reward for being part of the consensus algorithm.

There are two main kinds of tokens: Fungible tokens and Non-Fungible tokens (NFT).

4.1.1.1. Fungible tokens

Fungible tokens are divisible and non-unique. This means that it's possible to exchange a 1$ bill with another 1$ bill and the held value doesn't change. This reasoning applies the same for cryptocurrencies: 1 BTC can be exchanged with 1 BTC. The intrinsic value hasn't changed.

4.1.1.2. Non-Fungible tokens

Non-Fungible tokens are unique and indivisible. For example an airplane ticket is a non-fungible asset, since there can't be another plane ticket exactly equal to that one given the data embedded in it. With the same reasoning, it is possible to create non fungible tokens on blockchains that have data that make them unique.

In the token creation smart contract, the developer decides the total supply (finite or infinite), tokenomics, their emission and burning dynamics.

There are currently two standards that are being used the most for token creation:

- ERC 20 for fungible tokens
- ERC 721 for NFTs

We can also find ERC 777, ERC 1155, ERC 621, ERC 1400, ERC 1410, but they are used much less than the two above.

4.2.1. Tokens from a juridical point of view

Tokens in Europe, in Italy particularly, are classified in three ways:

- Payment tokens. They serve as a means of payment and are the synonyms of cryptocurrency. Bitcoin is the perfect example of this kind of token.
- Security tokens. They represent ownership of an asset and grant the token owners similar rights or equal to those of securities like voting rights, dividends, profit shares, etc. In terms of economic function, such tokens are security assets, assets (equity), debt (bonds) and liabilities. Security tokens derive their value from the underlying asset, however, the key difference is that as cryptographic tokens, they represent programmable ownership, giving assets more functionality, more liquidity, and easier market access, speed of creation, fewer (ideally none) intermediaries, lower costs for issuing, transparency and automated embedded safety processes.
- Utility tokens. They are used to provide access to an application or digital service. The access is exclusive to functionality within a decentralized network or platform. This type of

token is not designed for investments but by its definition it is of utility. They are comparable to vouchers and allow you to finance a project or company without diluting the ownership of that specific company/corporation

Tokens open up infinite possibilities for their applications: from art to financial assets, from housing to insurance, from concert tickets to weapons within a videogame and many more possibilities.

4.2. Blockchain properties and characteristics

4.2.1. Permissioned vs Permissionless

Blockchains can be permissioned or permissionless. In a permissioned blockchain, only those nodes that are approved by a semi-centralized or fully centralized authority can become part of the network as nodes and users. This solution is usually adopted by private companies that want to store their transactions and data on blockchain, where it is possible to regulate privacy, transparency, roles and many other traits. This kind of blockchain looks more like a standard database.

In a permissionless blockchain everyone can join and become a node, it will have to buy mining hardware or to invest its capital in order to participate into any other consensus algorithm. There are no requirements/limitations and the users can transact freely on the chain. In this kind of blockchains, all transactions are public, are censorship resistant and are not governed by a central authority, which in the end is the reason why Bitcoin and all other DLTs are born.

4.2.2. Blockchain trilemma

Blockchains' performances are usually evaluated on three main pillars: Decentralization, Security and Scalability. These characteristics are both strengths and weaknesses of a blockchain. In fact, Vitalik Buterin (Ethereum's co-founder) coined the term "trilemma": it is impossible (or very difficult) to solve and achieve maximum performance in all three of those properties, every blockchain will only ever be able to maximize two of those traits. [14]

The trilemma is basically the tradeoff between three properties: Decentralization, Security and Scalability.

- Decentralization is the property of not having a central authority that manages the chain.

- Security deals with the fact that if 50%+1 of all the nodes fall into a malevolent actor's hands, the blockchain could be corrupted, losing data coherence and users' funds.
- Scalability is the property of a blockchain to manage an increasing number of transactions as the adopters grow, without slowing down the transaction speed.

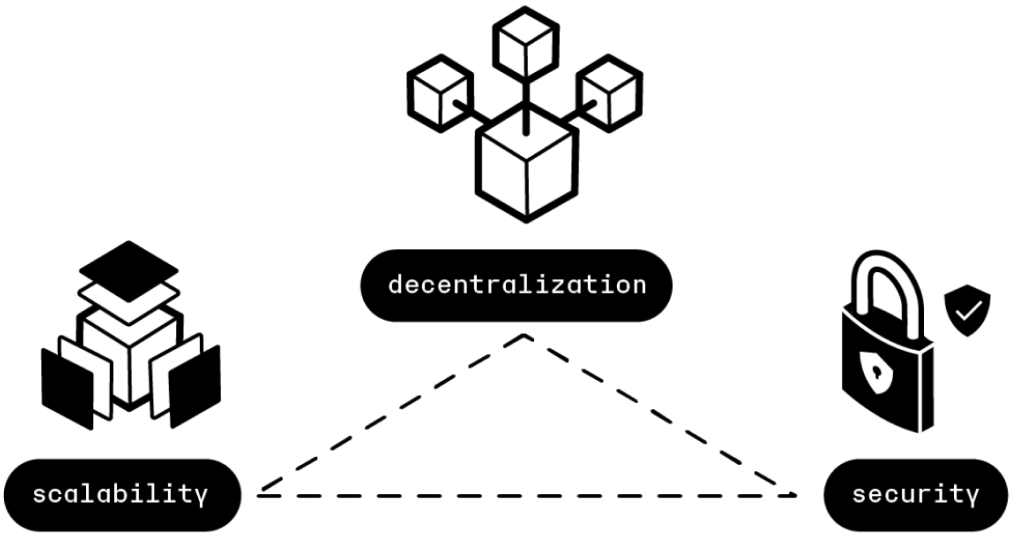

Figure 6. Blockchain trilemma

Usually blockchains concentrate on Decentralization and Security first: the more nodes are present, the more decentralized the ledger is and the more secure it will be, given the higher cost for a malevolent actor to own 50%+1 of the whole system. The more a blockchain gets adopted, the more transactions will be done on its network, leading to possible congestion given that each node can validate and mine a finite number of transactions and blocks in a time unit. [15] This would lead to having a much slower network and lower throughput of transactions than traditional payment methods: Consider that VISA can process 24.000 transactions per second, Mastercard 5.000, Cosmos (ATOM) can process up to 10.000, Ripple (XRP) 1.500 (but supposedly up to 50.000), Ethereum between 15 and 20 TPS, but with its recents switch from Proof of Work to Proof of Stake can potentially reach 100.00 TPS and Bitcoin can handle 7 TPS. In addition to slower transactions, with high network congestion, users would have to pay higher gas fees to the network in order to have their transaction processed before than other other users'.

To solve scalability a few solutions have arised [16]:

- Adopting a consensus algorithm that allows for a higher transaction throughput. This occurred recently with Ethereum when it went from PoW to PoS, where Ethereum's developers saw that switching to PoS would have brought improvements to the blockchain in terms of security, scalability and decentralization.
- Layer 2 solutions

4.2.3. Layer 2 as the solution to the scalability issue

Before defining what a Layer 2 (L2) is, Layer 1 (L1) must be defined first. As stated on ethereum.org "Layer 1 is the base blockchain. Ethereum and Bitcoin are both layer 1 blockchains because they are the underlying foundation that various layer 2 networks build on top of".

Ethereum as the layer 1 includes:

- A network of node operators to secure and validate the network
- A network of block producers
- The blockchain itself and the history of transaction data
- The consensus mechanism for the network

"A layer 2 is a separate blockchain solution that extends Ethereum and inherits the security guarantees of Ethereum." What does this mean in practical terms?

It means that the transactions are all done on the L2 solution, removing the burden of validating transactions and mining blocks from L1. Having these L2 solutions is basically like removing the scalability pillar from the trilemma, so L1s can concentrate on Decentralization and Security, whereas the L2s will concentrate on Scalability at the cost of Decentralization and Security. These Layer 2 solutions then store on the L1 the transaction data, not the transactions themselves. Having all the transactional data stored on the base layer, which is the most secure among the two, makes sure that the data recorded in the L2 is consistent and hasn't been compromised.

The most used Layer 2 solutions are [17]:

- Channels
- Sidechains
- Plasma
- Rollup

4.2.3.1. Channels

This Layer 2 solution creates a peer to peer channel where two parties can transact off the Layer 1 chain, not congesting it. They will keep transacting among each other until both decide to close the channel. The only two transactions that are recorded on the L1, are the transaction that creates the L2 channel and a final summary transaction that makes sure that the final balances reflect the transactions that were done in the channel.

Channels allow to take away transactions from the L1, which in turn leads to lower congestion, lower transaction fees and higher transaction speed on the L1 and higher transaction speed on the L2.

How do they work?

Two parties decide to open a channel by signing a smart contract so that they can do unlimited transactions among themselves, at higher speed and lower cost. They will both deposit money in the smart contract that creates the channel: the amount deposited by each member is the amount they will use to to transact plus a surplus that serves as an incentive of good behavior.

At this point they can start transacting unlimitedly (as long as the peers balances allow it) without any interaction on the Layer 1. If one of the two members behaves maliciously, all the funds locked in the contract go to the other. This serves as an incentive for good behavior within the channel.

When the two peers decide to close the channel, the closing transaction is recorded on the main chain and the summary transaction is done on the main chain, with the corresponding digital asset transfer.

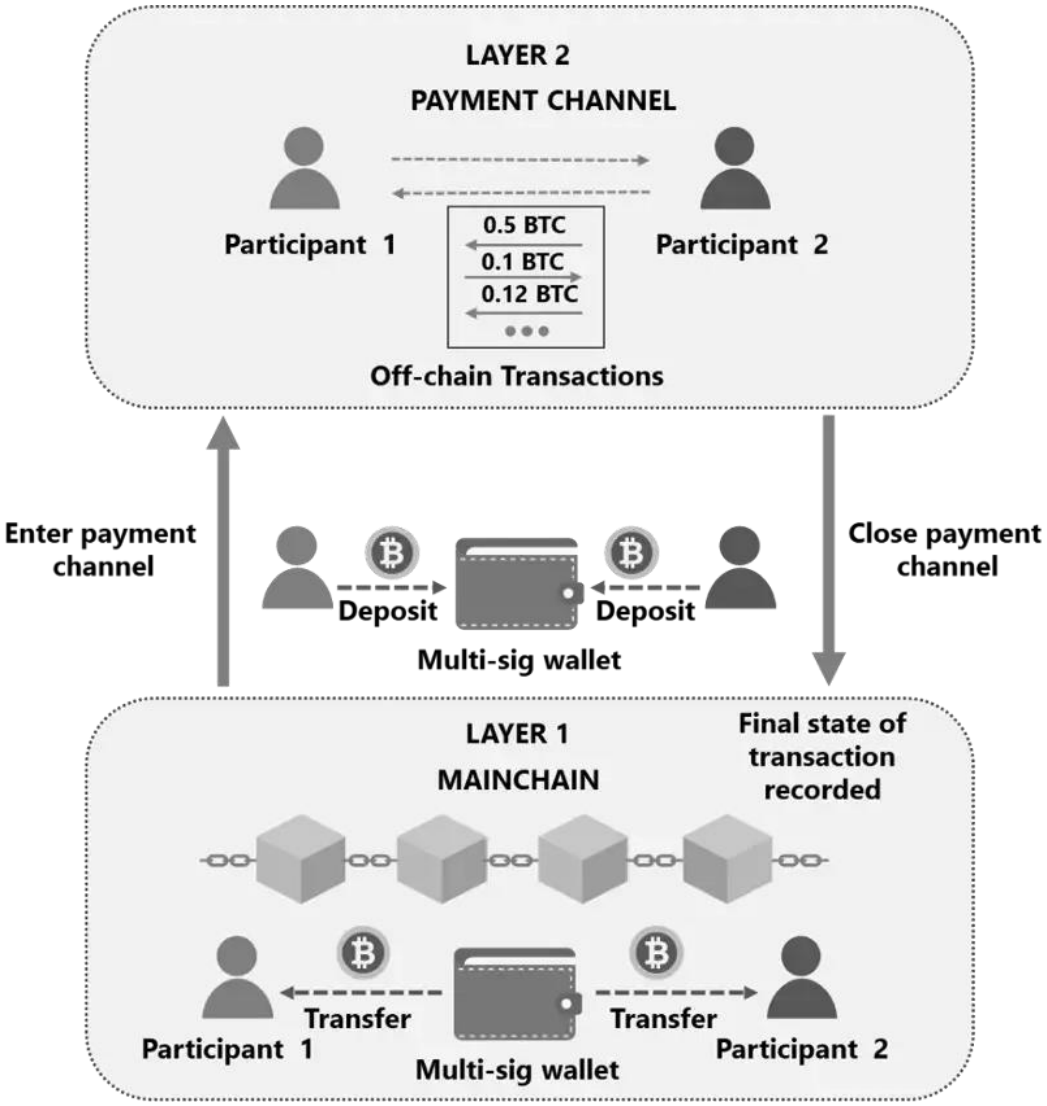

Figure 7. Channel's functioning

The problem of this solution is that it's not possible to implement smart-contracts within a channel.

An example of such a Layer 2 solution is Lightning Network developed on Bitcoin's blockchain.

4.2.3.2. Sidechains

"Sidechains are separate Blockchains that are connected to the main Blockchain through a two-way peg to help process some of the data from the main Blockchain."

Sidechains are fully-fledged blockchains that are linked to the Layer 1 blockchain, so they have their own rules, consensus algorithms, validation nodes but unlike other Layer 2 solutions, they don't rely on the main chain security, but they rely on their own on-chain security. Given that L2

sidechains are developed to have a high transaction speed, they usually have to trade it off having a more centralized network, given the relation highlighted by the trilemma.

Sidechain have three main characteristics/elements that allow them to function correctly:

- Two Way Peg (2WP)
- Presence of the third-party:
- SPV proofs

2WP

The 2 Way Peg is the mechanism that allows the passage of tokens between the main chain and the side chain: it allows for funds to be sent from one layer to the other. When a user wants to transfer his funds from L1 to L2, he will lock the desired amount in a smart contract (usually called bridge), which will in turn unlock the corresponding amount in the L2. The amount will stay locked in the bridging contract until the user wants to transfer its funds from the L2 to the L1. At this point the SPV comes into play.

Presence of the third-party

The third party is the party that deals with locking and unlocking the assets from L1 to L2 and vice versa. The fundamental role that the third party is given, is to make sure there is coherence between what is locked on one layer and unlocked subsequently on the other layer.

Given its importance in this kind of system, it may get too much power and authority leading to lose some of the decentralization that is reached within the L1.

SPV (Simple Payment Verification) proofs

They are a way to cryptographically prove that a given amount of tokens is locked on the main chain. SPV proofs check whether the locking transaction is valid and part of a valid block by comparing the hash of the transaction on the main chain recorded and the one calculated as SPV. If they coincide, then the tokens are unlocked on the main chain.

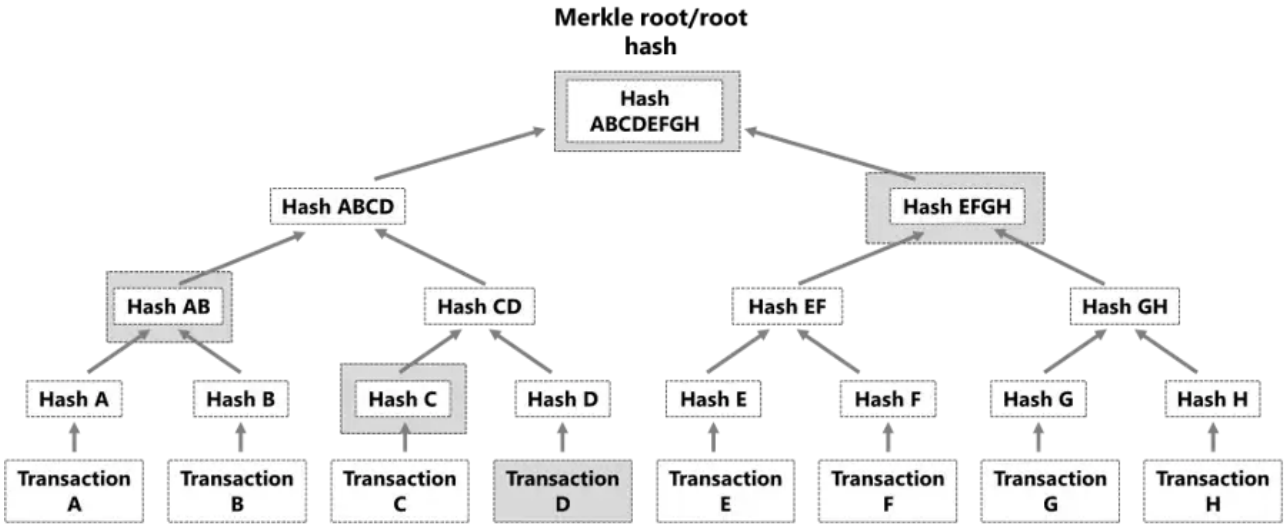

Figure 8. Merkle tree

So sidechains have both upsides and downsides: they increase transaction speed, decrease transaction costs, decongest the mainchain, but they are more centralized and less secure than the Layer 1, which goes against the founding decentralization principle of blockchain. On the other side, if the side chain is able to grow enough, it'll be able to reach a high number of validators that could ensure higher decentralization and security.

4.2.3.3. Plasma

Plasma employs smart contracts and Merkle trees in order to create many child chains that are the copy of the main chain. This permits to decrease congestion on the main chain. As for side chains, plasma chains have their own consensus mechanism, nodes, block size, and block time. But in this case security is assured from the main chain.

The child chain's smart contracts determine the rules of their functioning and act as a bridge allowing assets' transfers between main and child chain.

How do Plasma chains work?

First of all the plasma operator lays down the rules the child chains will operate, that make up the protocol of the plasma chain.

All the transactions stay on the child chain. Through its own consensus mechanism, the chain will generate new blocks. As said before, each block contains a Merkle root, a summary of the considered block's content. Each child chain's block header is posted on the main chain. This

widely decreases congestion on the main chain, since only the “summary” of each plasma chain block is recorded on the main chain, instead of all the transactions that are being simultaneously recorded on the child chains.

Data on the child chains are validated thanks to fraud proofs. Fraud proofs are a mechanism through which data can be challenged using Merkle proofs. If a fraud is happening, anyone can provide a fraud proof in order to prove that a given transaction is invalid. If the transaction is proved to be fraudulent, it is rolled back to the situation before the transaction.

Plasma chains are more secure than sidechains since they rely on the main chain’s security. They also allow the implementation of smart contracts and the possibility to transact with many users, whereas channels don’t allow smart contracts implementation and only allow for transactions among the two users that opened the channel.

On the dark side, when a user wants to transfer its assets from the child chain to the main chain, it may take up to 7/14 days for the transaction to be validated.

4.2.3.4. Rollup

This Layer 2 solution relies fully on the main chain, security included. In rollups, transactions that are started on the main chain, are then executed on the layer 2, bundled all together in a block that is then posted on the main chain. This solution takes away from the Layer 1 all the computational effort needed to validate transactions and is just left with having to add the blocks to the chain.

Looking at Ethereum’s case, rollups are enabled to run an EVM, this means that smart contracts can be implemented in this solution. Moreover, those smart contracts that run on the main chain can be “imported” by the rollups without having to write new code.

The advantage over plasma chains is that the whole transaction data is stored on the main chain, whereas with plasma solution, only the Merkle root of each block is recorded on the main chain. This feature gives rollups higher security with respect to plasma chains.

How do rollups work?

The rollup smart contract stores the state of the rollup layer. The state root of the rollup layer is the Merkle root of the current situation in the rollup, so it is the summary of all the transactions stored in the rollup. Every time new transactions are done in the rollup, the state has to be

updated on the main chain. In order to do this, the updated state root and the bundled up transactions are sent on to the rollup contract. The whole Merkle tree is then stored in the contract, not on the main chain.

Once the transactions are sent to the rollup contract, the transactions are stored on the main chain in a very compressed form, together with the previous state root and the updated state root.

The rollup contract then cross checks if the recorded state root is the same as the current state root and if they are equal, it updates its state root.

There are currently two main types of rollups:

- Optimistic Rollups
- Zero Knowledge Rollups (ZK Rollups)

Optimistic Rollups

As the name says, when a batch of transactions is posted on the main chain, it is not checked whether they are valid and not fraudulent. If a transaction is thought to be fraudulent, anyone can post a fraud proof. If it's demonstrated that a fraudulent transaction took place, the rollup rolls back all the batches until it gets to the last known valid batch.

So this kind of rollup assumes that all the transactions are valid and users must be wary that fraudulent transactions could be unnoticed and approved. They are more efficient because of the lower amount of needed computation, but provide lower security.

ZK Rollups

This kind of rollup instead has "Zero-Knowledge", so they always verify whether transactions are legit. This verification is done thanks to SNARKS (Succinct Non-interactive Argument of Knowledge), which verifies and gives proof that the new state proof is the correct result of the transactions on the rollup.

This gives much more security to the users since every batch is verified and proof is posted, but it has more computational effort.

Rollups are probably the most secure of the Layer 2 solutions that are available up to date, but since the transactions are posted on the main chain, they provide limited scalability. Moreover,

rollups come with an EVM, this means that when transactions are executed, users must pay transaction fees, which are present on every blockchain, but given the lower congestion, will be lower than those on the Layer 1.

Security, Decentralization and Scalability are for sure the three main pillars of blockchains and the dimensions on which they are evaluated. They are not anyway the only important characteristic.

4.2.4. Blockchain's environmental impact

Looking at secondary blockchain characteristics, the environmental impact is getting more and more relevance. This is another characteristic on which each blockchain tries to improve itself and use it as a differentiating element.

Consider that Bitcoin's PoW consumes on average 110 TWh/year, which is 0.55% of global electricity production (as per HBR), although it's estimated that around 60% of that energy is produced through renewable sources. [18] [19]

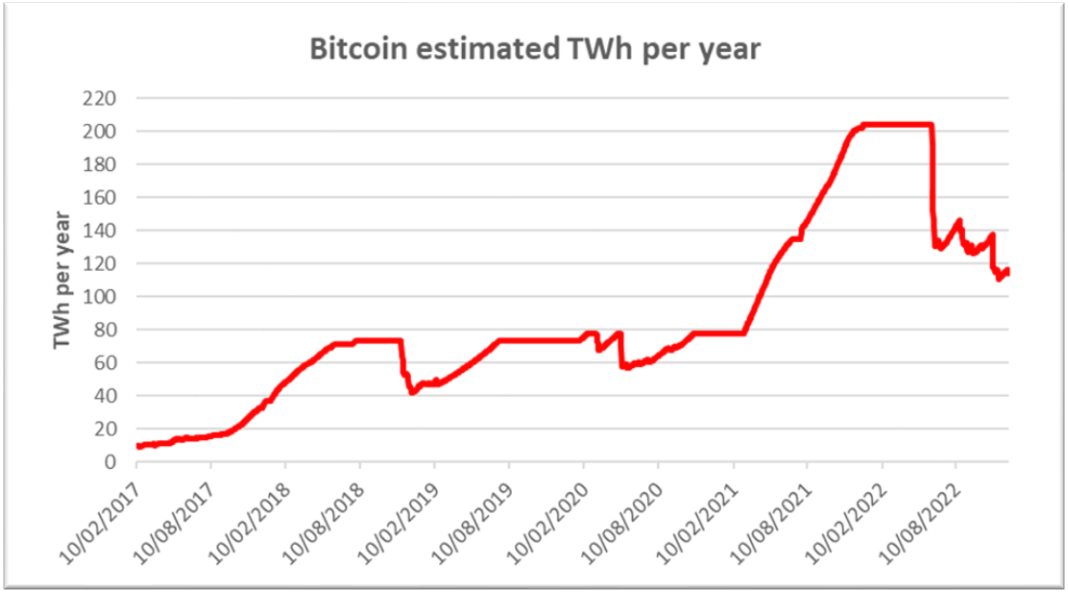

Figure 9. Bitcoin's energy consumption

Bitcoin's yearly footprint [20]:

- Carbon Footprint: 64,27 Mt CO2. Comparable to the carbon footprint of Serbia & Montenegro.

- Electrical Energy: 115,23 TWh. Comparable to the power consumption of the Netherlands.
- Electronic Waste: 40.96 kt. Comparable to the small IT equipment waste of the Netherlands.

Bitcoin's single transaction footprint:

- Carbon footprint: 673.31 kg CO2. Equivalent to the carbon footprint of 1,492,286 VISA transactions or 112,218 hours of watching Youtube.
- Electrical energy: 1207.17 KWh. Equivalent to the power consumption of an average U.S. household over 41.38 days.
- Electronic Waste: 450.10 g. Equivalent to the weight of 2.74 iPhones 12 or 0.92 iPads.

This relatively high consumption is given by the fact that Bitcoin's consensus mechanism, Proof of Work, is intrinsically inefficient because all nodes try to look for the nonce at the same time, which leads to competition among miners leading to increasing mining hardware investments, which in turn means higher energy consumption. Moreover, only the effort of one miner will have been enough to find the nonce, all other miners' work will be worthless and just resource consuming.

But it's exactly this inefficiency that makes Bitcoin so secure, since the high competition and high investments to enter make it not profitable to behave in a fraudulent manner.

Ethereum opposedly, switched from PoW to PoS on September 15th and went from an estimated 90TWh/yr to a 0,01TWh/year, decreasing its energy consumption by 99.8%. In the graphs below, it's possible to appreciate how the energy consumption went instantaneously decreased on September 15th when the switch from PoW to PoS occurred. [21]

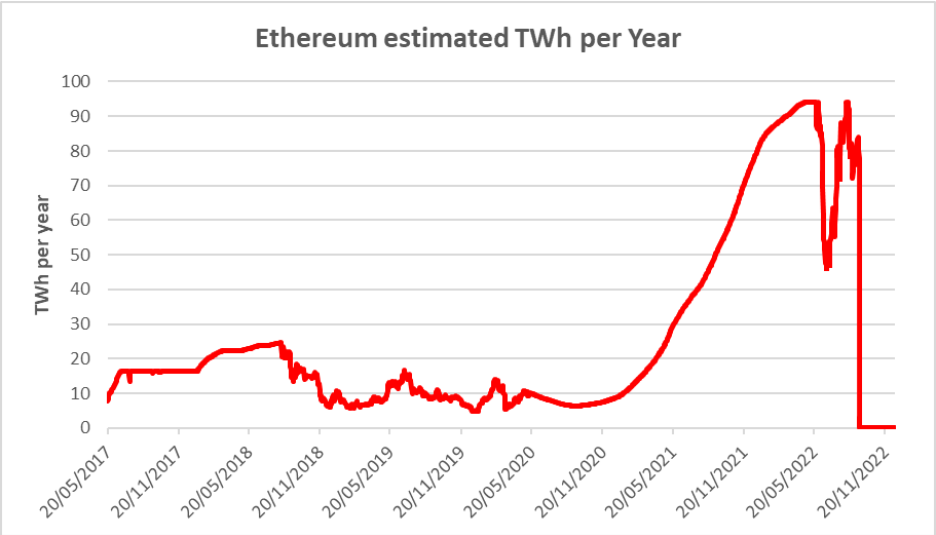

Figure 10. Ethereum's energy consumption

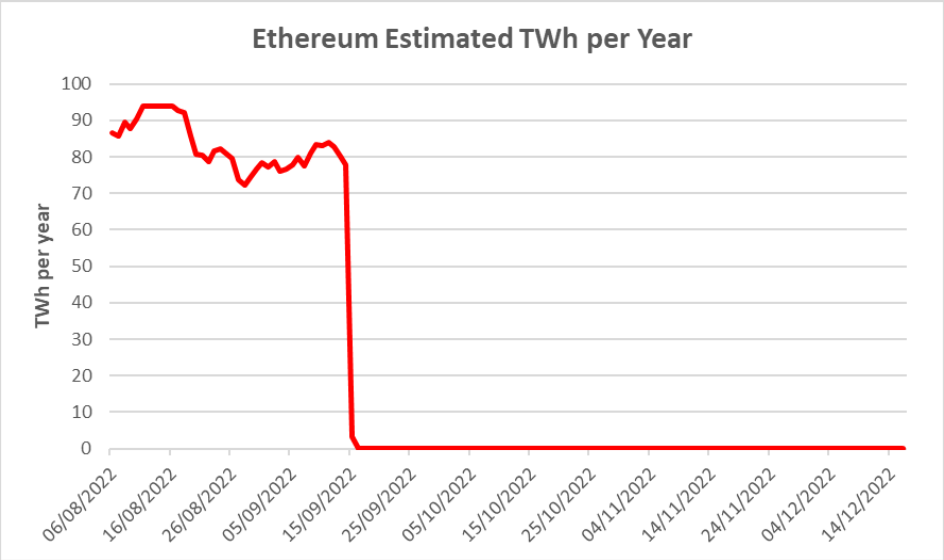

Figure 11. Ethereum's energy consumption

Ethereum yearly footprint, since switching to PoS:

- Electrical Energy: 0.01 TWh. Comparable to the power consumption of Gibraltar.
- Carbon Footprint: 0.01 Mt CO2. Comparable to the carbon footprint of Faroe Islands.

Ethereum per transaction footprint, since switching to PoS:

- Electrical Energy: 0.03 KWh. Equivalent to the power consumption of an average U.S. household over 0 days.

- Carbon Footprint: 0.02 kgCO2. Equivalent to the carbon footprint of 44 VISA transactions or 3 hours of watching Youtube.

Many other blockchains also have a near to zero carbon impact. A lower impact is possible when the consensus algorithm isn't reached by using computing power, but when staking or any other mechanisms that don't need energy consumption are used.

Below (Table 2 and Table 3), the comparison between Bitcoin and Ethereum environmental impact:

Yearly data	Bitcoin	Ethereum
Carbon Footprint [Mt CO2]	64,27	0,01
Electrical Energy [TWh]	115,23	0,01
Electronic Waste [Kt]	40,96	N/A

Table 3. Yearly comparison

Per transaction impact	Bitcoin	Ethereum
Carbon Footprint [kg CO2]	673,31	0,02
Electrical Energy [KWh]	1207,17	0,03
Electronic Waste [g]	450,1	N/A

Table 4. Per transaction impact

A 2021 report from Galaxy Digital compared Bitcoin's network consumption with that of banking and gold mining industries.

The aforementioned report calculated Bitcoin's energy consumption and compared it to that of other industries.

Bitcoin consumes 113,89 TWh per year, while the banking industry consumes 263,72 TWh per year. To arrive to this (estimated) value, Galaxy Digital considered the energy consumption of the following components of banking:

- banking data centers,
- bank branches,
- ATMs,
- card network's data centers.

Bitcoin's energy consumption is for sure not negligible, but as stated before, it's the high level of consumed resources and inefficiencies that make it so secure.

Moreover, Galaxy Digital compared Bitcoin's energy consumption with the gold industry too since bitcoin is often referred to as digital gold. The gold industry has an estimate consumption between 263,72 TWh and 240,61 TWh whereas Bitcoin consumes 113,89 TWh. [22] [23]

5. Blockchain diffusion and applications

Up to now the blockchain's general functioning has been dealt with, but the technology diffusion trends and current applications haven't been mentioned yet.

Blockchain technology was originally born as peer-to-peer digital money, so it had the "only" purpose to allow value exchange in a trustless and decentralized way, that allowed to cut out the middle man from transactions. With the advent of Gen2 blockchains and smart contracts, it became much more than an alternative to traditional money exchanging methods.

Just like every new technology that is at the beginning of its development and adoption process, there are currently many fields of application that are being tested: housing market, financial market, art, supply chain, digital identity among many others. As it usually happens, many of these applications will fail (or have already failed) over time because they won't be appreciated by the market. For this reason, the blockchain industry will turn its attention towards those applications that are the most valuable for users and profitable for companies.

Let's now look at blockchain's diffusion dynamics and try to formulate a prediction on future trends.

5.1. PEST analysis

In order to look at an innovative technology's diffusion, the environment where it is developing and evolving must be outlined first. A useful tool to do so is the so-called PEST (Political, Economic, Social, Technology) analysis. Note that some points are repeated in different fields. [25]

Political:

- Government institutions are seeing blockchains used as a payment channel as a threat, since it takes away "power" from Central Banks, given its decentralized nature.
- Central authorities are also afraid of not being able to help the economy recover in case of a recession, if the circulating currency isn't under their direct control.
- The worldwide normative framework isn't clear and well defined yet. Many Governments are working on creating clear laws on how to deal with crypto assets and how they should be taxed.
- Some Countries have already declared cryptocurrency as a payment channel. El Salvador, South Africa, Slovenia and Switzerland are some of the examples.

Economical

- Blockchain is receiving a lot of attention from different industries, so investments are coming in from very different fields.
- Crypto currencies' prices are subject to volatility, and when prices are low, also investments in the sector decrease because the blockchain technology is seen as less attractive although it's cheaper to enter, so failure is less costly.
- Banks see blockchains both as a threat and an opportunity. Banks won't be central as they have always been if blockchain becomes a worldwide technology. For this reason banks have been investing in creating their own blockchains and cryptocurrencies in order to retain some of that power.
- Blockchain enables new financing forms, potentially making capital more accessible for firms/companies of every size.
- Cryptocurrencies (Bitcoin especially) are being used as an inflation shield in very high inflation countries.
- Cryptocurrencies and crypto wallets allow the unbanked part of society (Third World countries mostly) to have a way of managing their funds.
- Blockchain currently has a Market Capitalization of 4,9 billion $, and is expected to grow to 67,4 billion $ in 2026, with a CAGR of 68.4%. [24]

Social

- Blockchain is still seen as a "monster" only used to invest in crypto currencies and not for its decentralized trait.
- Enhance trust between individuals thanks to the trustlessness of blockchain.
- Cryptocurrencies (Bitcoin especially) are being used as an inflation shield in very high inflation countries.
- Cryptocurrencies and crypto wallets allow the unbanked part of society (Third World countries mostly) to have a way of managing their funds.
- Blockchain empowers individuals that are the only owners of their funds.

Technology

- Still in the development phases, where the technology is improving, but each application's dominant design is yet to be found.
- Blockchain could enhance and be enhanced by other complementary technologies, like NFC (Near Field Communication) or IoT.
- Having a clear regulation on how to deal with cryptocurrencies and crypto assets in general would allow a faster adoption and expansion.
- Blockchain can be implemented in many industries, each one of them will have to find the best way to implement this technology.
- There is still a lot of misinformation about this technology.
- A killer app hasn't been found yet.

5.2. Patents and investments

Other helpful innovation diffusion indicators are the number of patent filings over time (for which data is available up to mid april 2019) and blockchain related investments. Looking at the graphs below, it's possible to notice an increasing trend in both. This is a sign that more and more actors are getting interested and are seeing value in this new technology. Regarding the investments' data, waiting for the whole 2022's data, it is possible that investments didn't increase, given the high geo-political instability and very stringent monetary policies. The next years' macro economic and political event will for sure determine if and how fast blockchain will become a widespread technology.

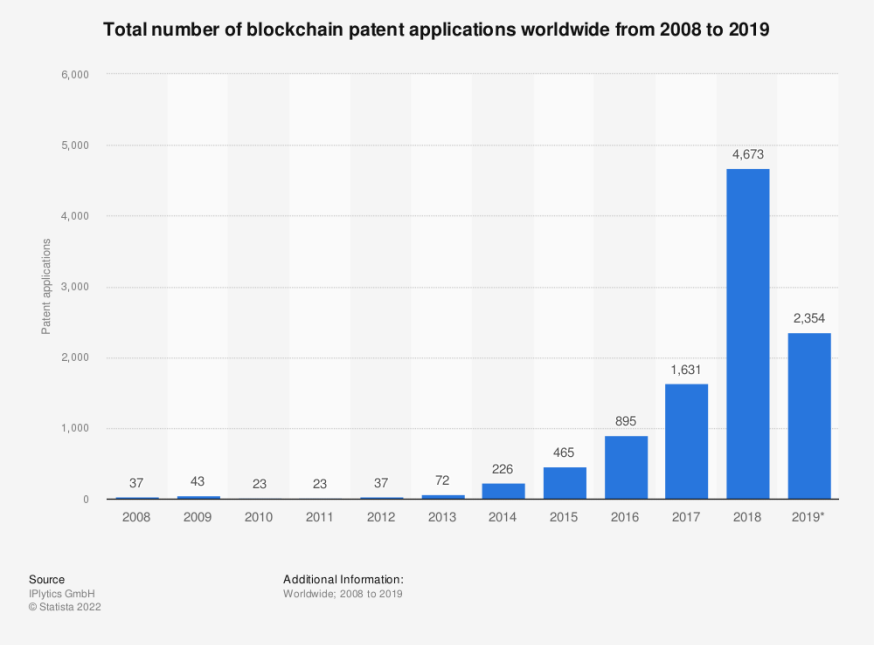

Figure 12. Total number of blockchain patent applications from 2008 to 2019

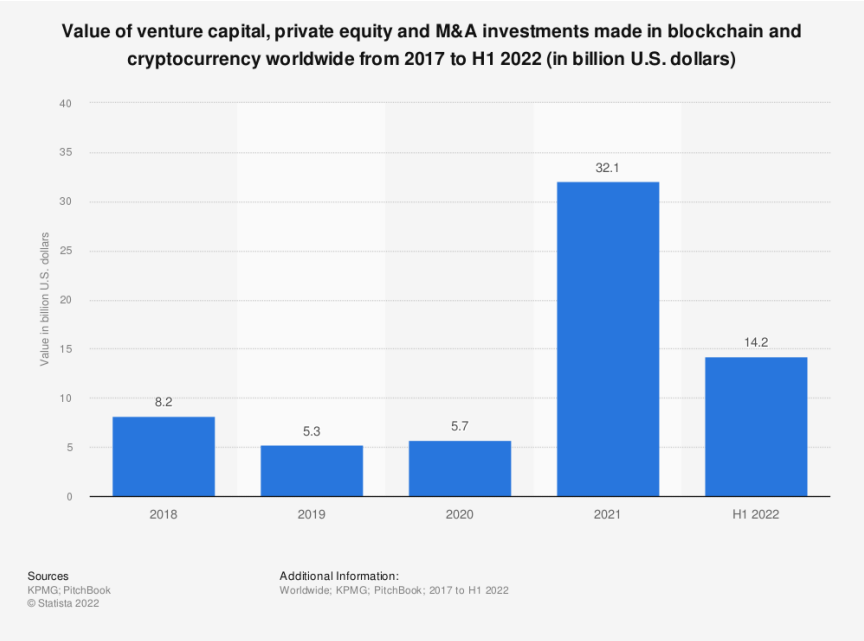

Figure 13. Investments made in blockchain and cryptocurrency from 2017 to H1 2022

5.3. Hype cycles

Continuing with a deeper analysis of new technologies' diffusion dynamics, a pattern in an innovative technology's diffusion can usually be found.

In the starting phases of the technology's development, many firms from different industries enter the market and try to find the application they think best suits users and themselves. After being in the market for some time, trying to grow within the market and improve their product, the firms that didn't develop a solution that was appreciated by the market will fail and exit the industry. The firms that instead developed a solution that was appreciated by the users, will stay in the market and will hire people from the failed companies to gain market insights and experience. The phenomenon of firms exiting the market is called industry shake out.

Adopting Gartner's hype cycle as a framework to analyze the technology's development stage, the hype cycles from 2018 and 2022 have been taken into consideration. Hype cycles give a view on the level of expectations about a given technology and its applications, they don't give a clear insight on the diffusion state of the technology. Given the level of expectations, it is possible to understand at a high level if a technology is still in the early phases of diffusion or if it is already maturing and going towards mass adoption.

Looking at the hype cycles below (Figure 14 and 15), it is reasonable to state that the "average" application is now transitioning from the inflated expectations stage, where a large number of firms and applications come up, to the trough of disillusionment where the non-successful applications fail and the market goes through the shake out. After this phase, the technology will enter the slope of enlightenment, where the most resilient and best applications for each industry will become dominant designs and will start diffusing more and more among users and industries. The technology will then reach the plateau of productivity where the technology becomes widely implemented, its applications are well defined and have a precise position and role in the market.

2018 BLOCKCHAIN HYPE CYCLE

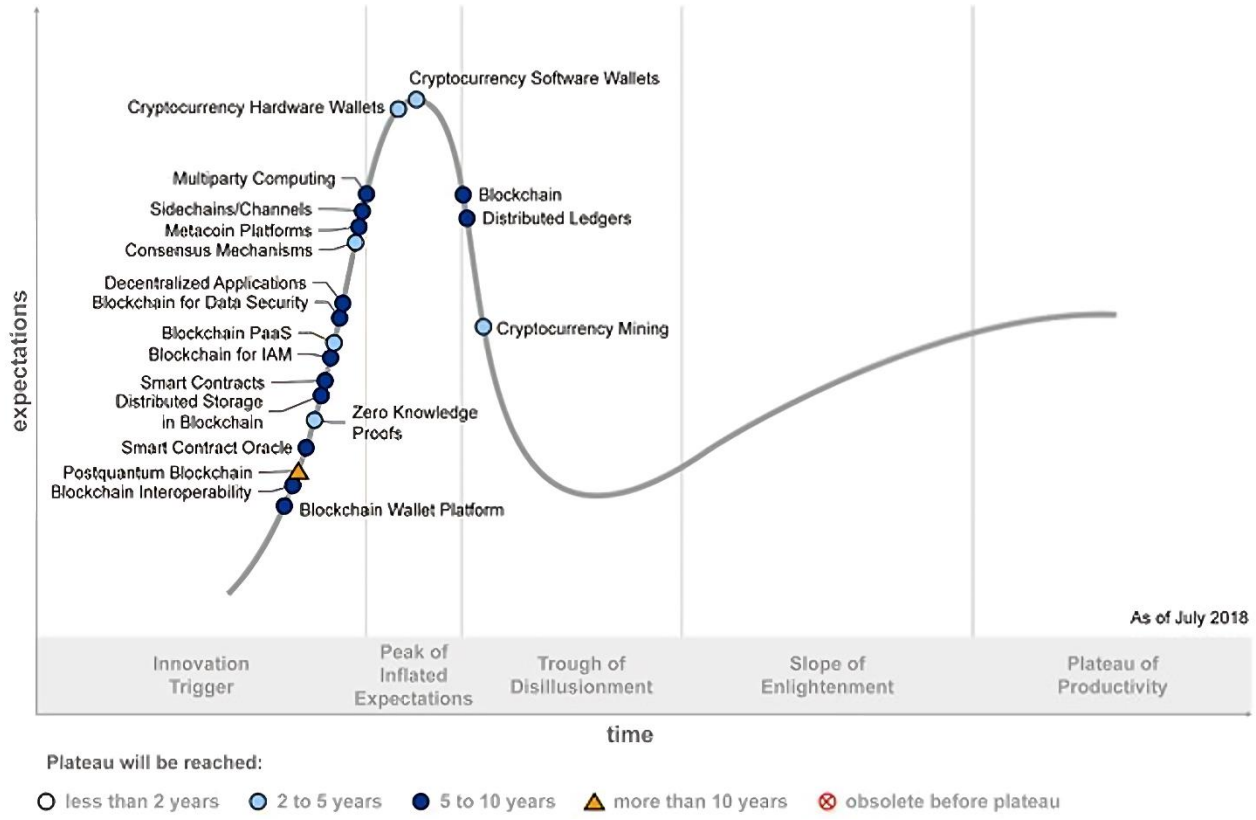

Figure 14. 2018 Blockchain hype cycle

2022 BLOCKCHAIN HYPE CYCLE

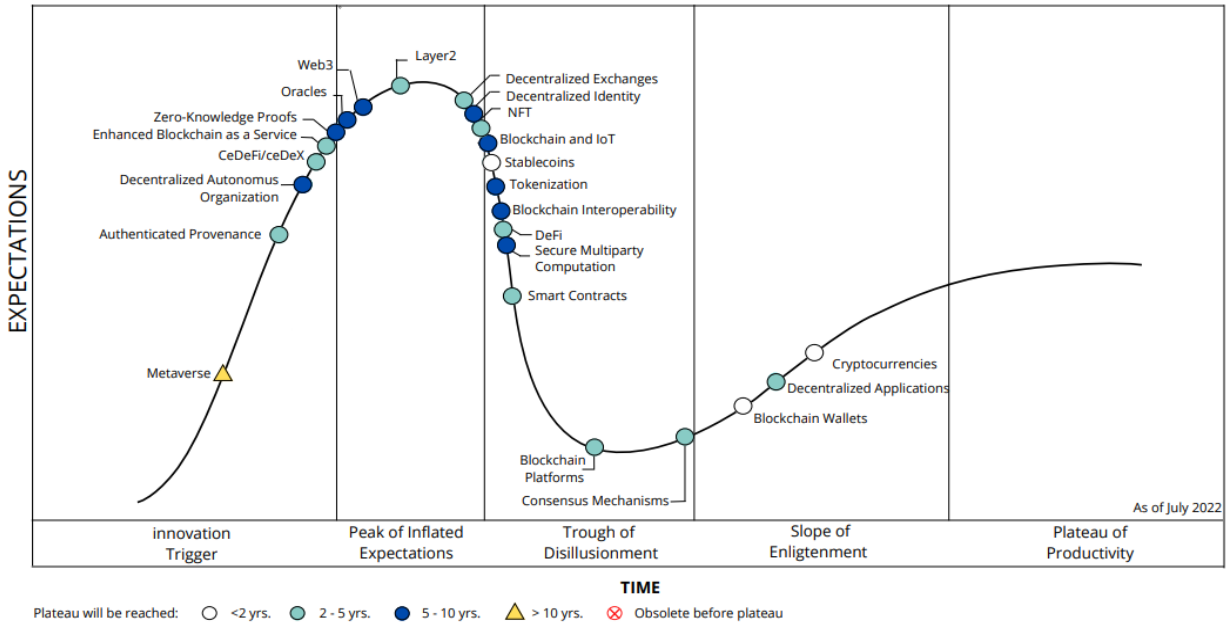

Figure 15. 2022 Blockchain hype cycle

5.4. Internet vs Blockchain

In order to check for the penetration of blockchain technology within the population, blockchain technology was compared to the diffusion slope of one of the most disruptive technologies: the Internet. Blockchain has the potential to be a disruptive innovation too. The graphs below (figure 16 and 17) show the diffusion of the Internet versus the diffusion of blockchain, measured by millions of users. Consider that blockchain's slope has been "normalized" to 1995 when the internet was born, in order to have a year by year comparison (1995 corresponds to 2016 for blockchain's timeline). [26] [27]

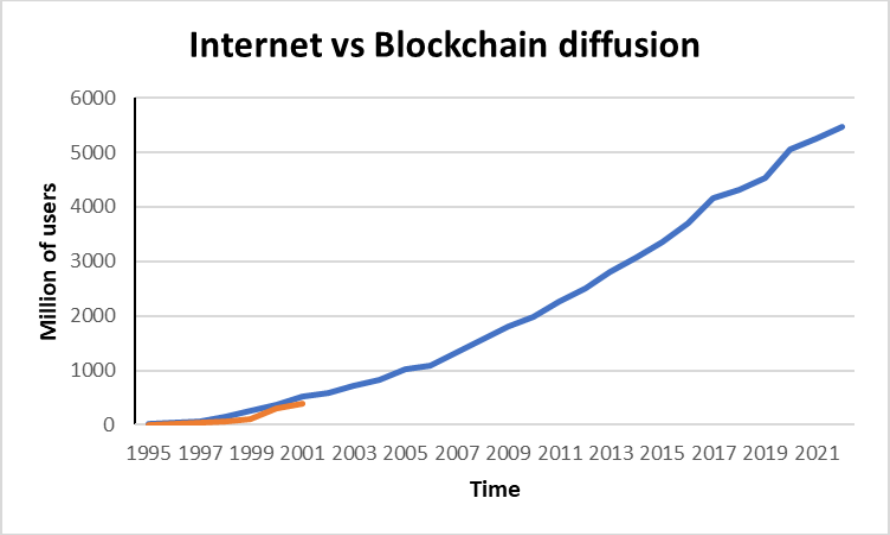

Figure 16. Internet vs Blockchain diffusion

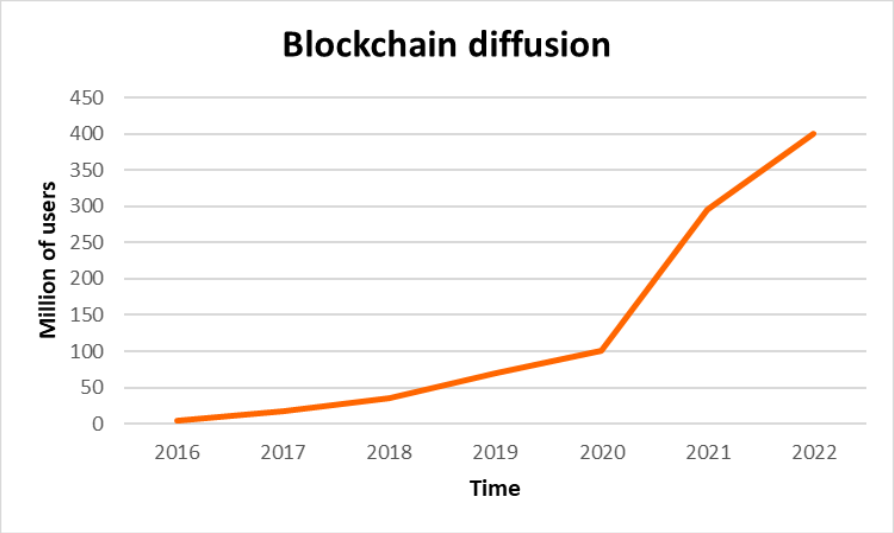

Figure 17. Blockchain diffusion

There are some similarities among the two curves. Blockchain's curve is fluctuating more, although always increasing. This is possibly occurring because blockchain's diffusion is strongly influenced by the price of the underlying crypto currencies: when prices and evaluations are higher, more people start getting interested in this technology, seeing it as an interesting investment opportunity. Moreover, holding cryptocurrencies have the risk/benefit of large price fluctuations.

This has occurred in 2021 when the crypto currencies market reached an all time high evaluation of 3,000 billion dollars, corresponding to a peak in adoption. It's possible to see this same effect, in a more mitigated way in 2018 too, when the market reached an evaluation of 760 billion dollars and the diffusion increased.

The Internet was different from this point of view: although costs for an internet connection and a computer were high, users wouldn't see any loss in value in their investment (not considering the computer's devaluation over time). So getting started with the Internet was possibly more easy from a psychological point of view, since the cost would be an a-tantum and then would become a sunk cost. [28]

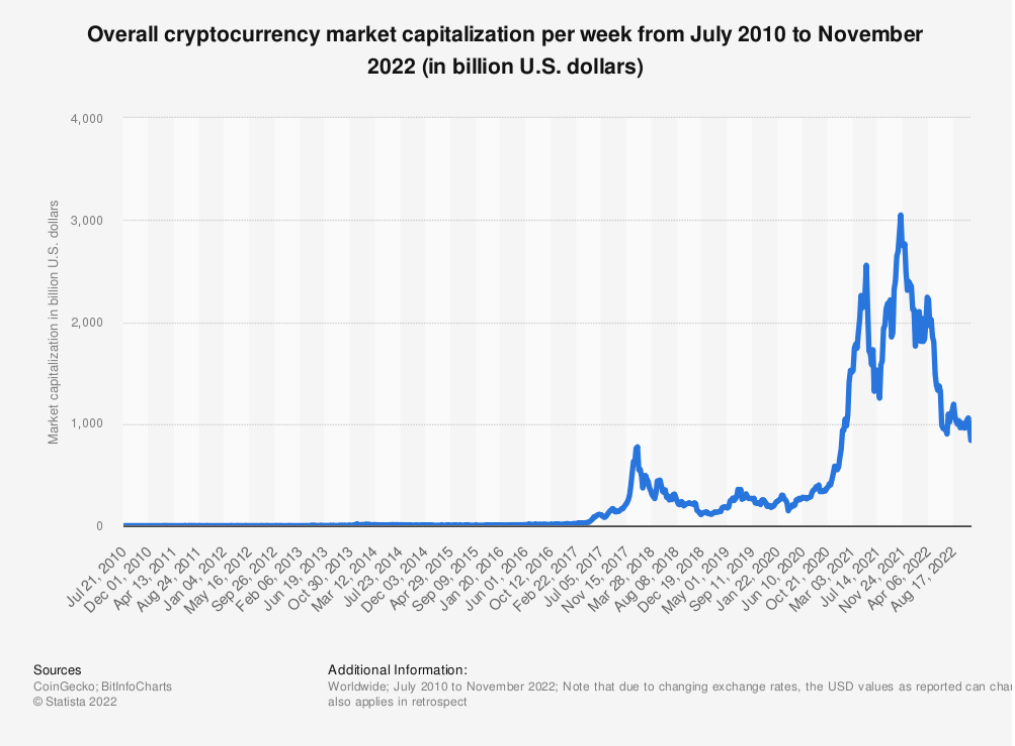

Figure 18. Total cryptocurrency market capitalization

5.5. Roger's adoption model

To conclude, looking at the graphs above, it's possible to make a good estimate of the diffusion stage blockchain technology is in: total internet users are 5.473 million, whereas blockchain users are roughly 400 million. This means that roughly 7,3 % of total potential blockchain users have already adopted this new technology. Looking at Roger's diffusion model below, it's possible to

conclude the technology is currently being adopted from the early adopters. Up next there will be adoption from the early majority: the passage of adoption from the early adopters to the early majority is called the chasm. If a technology can't successfully transit through the chasm, the technology will not become mass adopted, and will either die or just be used by a niche of the potential adopters.

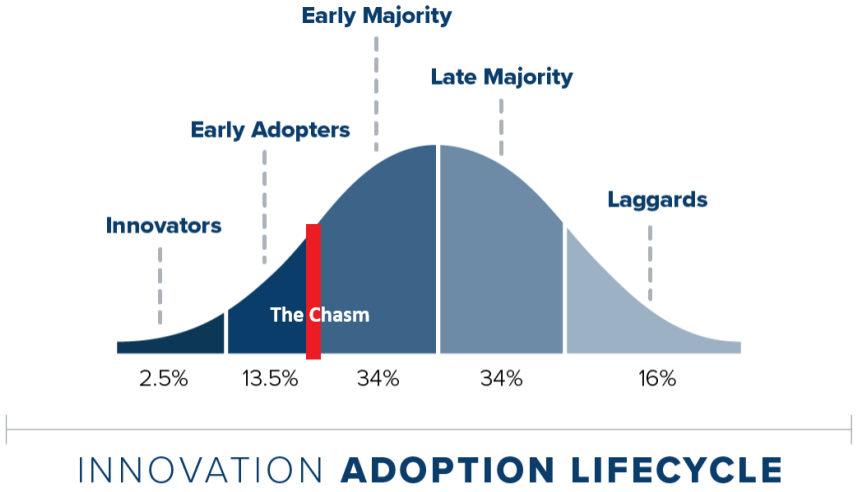

Figure 19. Roger's adoption model

5.6. Current blockchain applications

Given the stage of evolution of blockchain technology, many applications of blockchains are being tested at the moment. Some of them will be listed below.

5.6.1. Money transfer

This will be the only application that will potentially never die, given that blockchain was created to allow the transferring of value between people without the need of an intermediary. As stated before, the scalability issue must be solved or mitigated at least in order for this application to become as cost efficient as it is with current traditional money transferring methods, but money transfer is being employed nowadays especially for cross-border transactions.

It's already possible and common practice to pay with Bitcoin in South Africa and in El Salvador, which has been actively investing in Bitcoin including it as part of the National Treasury.

5.6.2. Lending/Borrowing

This application is part of a branch called De-Fi, or Decentralized Finance. Thanks to smart contracts, called protocols, it is possible for users to ask for loans. The process is much faster than traditional lending and with lower transaction costs.

The process has three stages:

- the users signs a smart contract that locks an asset as a collateral
- the smart contract gives the loan in crypto currencies. Usually the loan is a percentage of the collateral value, making it an overcollateralized loan. This is an incentive for the user to payback the loan.
- Once the loan plus interest is paid back, the collateral is released from the contract and returned to the user. If the ratio between loan and the collateral rises above a given value, the collateral is sold in order for the protocol to mitigate the risk of having an undercollateralized loan.

Example. Elia has 100.000 $ worth of Ether and needs a loan in USD. The protocol will require a collateral higher than the value asked as a loan. Let's suppose the protocol gives up to 80% of the collateral value. Elia will sign a smart contract that will lock its 100.000$ in ETH giving him 80.000$ against a collateral of 100.000$. By design, the protocol states that if

$$\boldsymbol{TVL\ (Total\ Value\ Locked)} = \frac{\$\ \boldsymbol{value\ of\ loan}}{\$\ \boldsymbol{value\ of\ collateral}}$$

goes above 90%, the protocol automatically liquidates Elia's debt. If that occurs, the protocol will sell the collateral in order to cover the loan and Elia will keep its 80.000$ loan.

If instead the TVL doesn't go above the threshold, once Elia pays back its debt, he will receive back its 100.000 ETH collateral.

These kinds of loans are currently being done also for "traditional" businesses. The company has an invoice that it knows will be paid in 60 days, but needs liquidity right now. Protocols allow for the company to put the invoice as an over-collateral and the company will immediately receive the loan as a percentage of the invoice's value. The company will then have to pay back the loan within the agreed terms or the protocol will cash in the invoice. This application requires banks in the picture as actors, but in this case they are not involved with the actual loan, they are just the means through which the liquidation occurs.

5.6.3. Art

Thanks to tokens, it is possible to allow multiple benefits for the art sector:

- Thanks to NFTs, that are non replicable and non-divisible, it's possible to univocally attribute a piece of art to its true owner. This would make counterfeiting much more difficult.
- Given that tokens are on the blockchain, this also enables buying and selling art without the need for third party involvement. ensure that only one copy exists.
- Again, since tokens are on the blockchain and that blockchain transactions are public, it is very easy to track ownership of a token and its "ownership history".

Considering then the artists' point of view, thanks to tokens and smart contracts, it is possible for them to receive royalties on each sale. This allows artists that were not famous at first (meaning that they sold their art at a "low" price) to get recognition and receive a payoff for their work when one of their art pieces is sold at an extraordinary price.

5.6.4. Insurance

Through blockchain, it is possible to record data of a customer, the number of claims that were made, the reason for which they were made and much more information. This would allow both insurance companies and users to establish a fair amount for their insurance premium. This would be possible also thanks to the Internet of Things, that could record data of speed, acceleration, km per day and any other significant data for a car (in case of a car insurance) and the company thanks to that could determine the insurance premium, based on actual data.

Alfa Romeo created the Tonale NFT, based on blockchain technology and uniquely linked to one car each, certifies the car upon purchase, records essential vehicle data, and generates a certificate that can be used to ensure the car has been properly maintained during its life cycle, with a positive view of protecting its residual value. This could be useful for both insurance and second-hand market dynamics.

5.6.5. Real Estate

Given that with blockchain establishing who the owner of an assets is fairly simple and straightforward, using it in real estate transactions could be a smart application. Transacting on

blockchain would decrease transaction costs (time, paperwork, background checks) and would make it much easier to manage real estate property.

5.6.6. Healthcare

In the healthcare field, patient's data is one of the most valuable and at risk elements. That's why blockchain could allow safe transfer of sensible medical information between doctors and/or institutions, reducing the risk of data leaks and hacks.

5.6.7. Digital Identity

Nowadays, there is a (very) strong trust relationship between internet users and internet platforms like Google, Facebook, Amazon among many many others. Users trust these entities into storing their personal information, like passwords, credit card numbers, home addresses and personal information. These big players then sell users' data for a profit, without asking the users' permission. The users in this centralized model of data management are not actual owners of their data

With blockchain, the users would remove power from these institutions and become the actual owners of their data. The institutions that emit certifications and/or identity documents could send the documents to the users' wallet. Those documents would then be regarded as legit and authentic since the institutions' wallets are public.

Digital identity would also allow for that part of the world population, that is around 1.1 billion people, where physical personal documents are not available, to have all that data available in a digitized and easily accessible manner. [29]

5.6.8. Asset tokenization

Assets tokenization is the process of the creation of tokens tied to real assets. The tokens are created on the blockchain through the means of a smart contract.

Asset tokenization employment and wide diffusion (although its use is currently limited both by the fear of new technologies and non clear regulations) may lead to numerous benefits, among which lowering costs, higher transactional efficiency, higher transparency, higher potential market liquidity given that even small investors would be allowed to invest where they would most likely be excluded in traditional finance.

Asset tokenization represents pre-existing real assets on a blockchain, by assigning or including the rights and the economic value of the tokenized real assets to the tokens and for the transitive property to the token holders. Tokens used to transfer value and rights of real assets on the blockchain, logically require that the tokenized real asset keeps existing off-chain, or else they would lose value and the rights tied to that asset. This means that the real asset should be stored in safe custody to make sure that it continues to exist, constantly backing the value and rights of the corresponding tokens.

Considering securities as the real assets taken into consideration, their corresponding tokens can be considered as dematerialised securities that are stored and recorded on the blockchain, instead of the traditional securities registers of central (and centralized) securities depositories. One of the disruptions this blockchain application would bring, is that, since securities would now be decentralized and smart contracts would allow to automatically settle transactions, there would not be the need for a trusted third party (in theory). Thanks to smart contracts, intermediaries involved in dividends distribution or in voting processes wouldn't be needed anymore.

Using blockchain for asset tokenization could deliver higher efficiency in terms of costs and time, without having to rely on a centralized party, leading to lower transaction costs, lower friction among all the actors involved and lower costs for monetary transfers. Thanks to smart contracts, the main corporate actions, like dividend payments and voting, would be facilitated, and the overall operational transparency would be enhanced. Moreover, issuing tokens on the blockchain would allow the emitting party to have full control over the whole token supply, meaning easier management of the whole "investment environment" from the creation to the destruction (if planned) or the maintenance of the security but higher risk in case the emittent gets compromised and its actions become malevolent.

This application would not only bring an increase in overall transactional efficiency given its decentralized nature, but, since blockchains are public, it would lead to increased transparency about the issuer itself, the tokens' characteristics and transactional data.

Expanding the point of view to the whole financial market, asset tokenization would probably bring benefits in the form of data integrity, immutability and security. This would be enabled by the decentralization of blockchain technology, that leads to not having one single point of failure. A higher level of transparency could be also reached in terms of compliance and regulators: thanks to smart contracts, regulations can be automatically enforced and the regulator would only get

notified in case of breach of the rules. Blockchain would also allow regulators and any interested entity to have a close to real time overview of the information about on-chain events.

Even though blockchain enables a high level of transactional and informational transparency, the "garbage in, garbage out" principle applies. This would lead to a distributed, immutable and transparent register of uncorrect data. To solve this problem either regulated entities validate data, but at that point the un-censorship trait of blockchain is lost, or oracles should be involved, that are actors that automatically take data from the real world and put it onto blockchain. Probably the more blockchain will be used, the higher the amount of data to be relied upon and used, in order to create a creditable register of data.

Through asset tokenization, it's possible to fractionalize ownership, allowing a higher number of small and retail investors to enter the financial market, increasing the amount of potential capital circulating in the market. For example, usually SMEs (Small-Medium sized companies) are actors which can issue debt/equity capital securities, but they are usually only reserved for institutional investors.

Asset tokenization doesn't only enhance inclusiveness on the investors' side, but also on the issuers' side. For SMEs, it's often very burdening to try to seek capital in different ways than traditional bank loans. With asset tokenization, any kind of investor (after the necessary and opportune checks) could invest and fund SMEs, allowing for a more efficient capital allocation within the economy. SME increased access to alternative financing forms could be enhanced by the possibility of tokenizing illiquid assets, making them a source of funding.

To sum up, no matter if we're dealing with financial assets (i.e. bonds, shares) or real assets (i.e. houses, warehouses, power plants, ecc…), the tokenization of these assets has two major upsides:

- lower transaction costs, higher transaction speed, easier traceability, no third party involved
- possibility to fractionalize each asset in multiple other assets, opening the market to a larger base of investors

To provide a short example, in 2019, a villa in Paris that was at the time valued at 6.5 million euros was tokenized and put on the Ethereum blockchain. The asset was then divided into 1 million pieces (tokens) of as small as 6.5 euros (meaning that to buy one token, you had to pay 6.5 euros). This solution allowed to have both an easier way of raising capital and to have a larger investor

base. The investors would then profit from an increase in the value of the underlying asset and from any other use of the villa (like rent for example).

6. WAREHOUSE TOKENIZATION

As stated in the title, a very specific blockchain application will be analyzed, trying to give the most complete overview on the different points of view of the actors involved: warehouse tokenization for Parmigiano Reggiano cheese producers.

First of all, why such a specific application?

In April of 2022, I won a scholarship for a blockchain focused course: “MasterZ Blockchain and digital assets course”. In order to obtain the certification of participation, together with some partners, they asked participants to develop some project work. Me and my group developed a project work in partnership with Crédit Agricole and BlockInvest. The request was to create a “Basic design of a fintech project on tokenizing real world financial assets, focusing on bonds, real estate and warehouse tokenization. Your goal is searching for traditional illiquid financial assets and drawing new sell/buy flow, using Blockchain technology, in order to make them liquid and tradable.”

A couple of members from our team are from Emilia-Romagna region, so they proposed a topic that had to do with their specific region typical production.

6.1. Problem Parmigiano Reggiano producers face

Parmigiano Reggiano wheels must age in order for them to become the renowned product it is around the world.

The process of aging cheese wheels leads to having large amounts of capital locked in the aging warehouse. Consider that producers usually age wheels up to 36/40 months. Moreover, wholesalers buy large stock of wheels from the smaller producers, age the wheels themselves, and then sell the wheels, receiving all the credit for the quality of the product and profiting from the increase in value given from the aging, taking away that possibility from the smaller producers.

With this industry dynamic, the wholesalers are the only players that get recognized for their work and small producers don’t have the possibility to grow and become big players themselves.

6.2. Proposed solution

In order to make the aging cheese stock a liquid asset, a producer could tokenize part of its warehouse, so each token would represent a “share” of the producer’s warehouse. By buying these tokens, investors would finance the producer with liquidity that can be invested by the

producer to either increase its productivity, storing capacity or any way the producer seems fit. The investors would then get a share of the increase in value (given by the cheese aging) of the tokenized warehouse.

By creating this new financial instrument, a traditionally very illiquid asset such as aging cheese warehouse stock, would become much more liquid. Not only that, but a secondary market for these new security tokens could develop.

6.3. Parmigiano Reggiano market

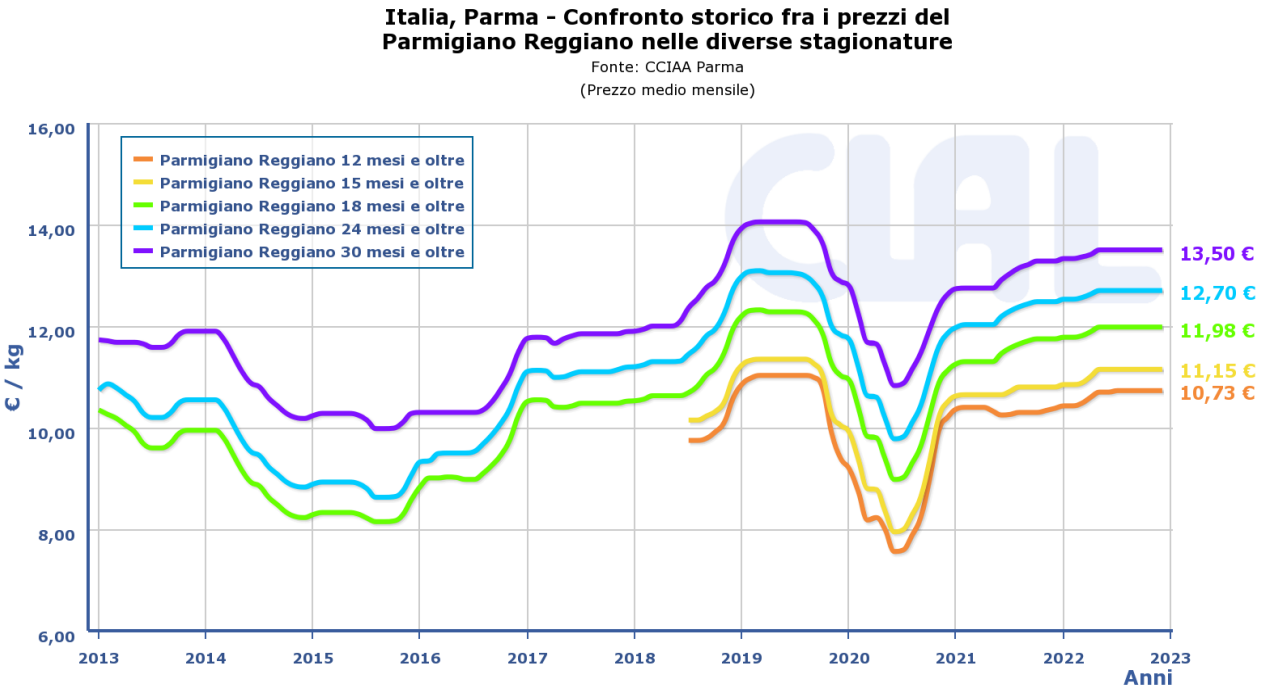

Figure 20. Comparison of prices for differently aged Parmigiano Reggiano wheels [30]

Prices of Parmigiano Reggiano have seen an increasing trend, meaning that it is a market in good health, the fame of this product is spreading all over the world and producers may be willing to invest in their equipment in order to increase their productive efficiency and/or storing capacity. In order to do so, they might look for alternative funding solutions, for example tokenizing part of their warehouse in order to receive liquidity. The recent energy crisis and increase in price might put producers' profits at risk, for this reason too they might be willing to invest into higher efficiency processes, to cut down overhead costs.

6.4. Producers' warehouse analysis

From January 2022 up to December 2022, a total amount of 4.002.270 wheels have been produced from a total of 295 producers, meaning that on average each producer produced 13.567 wheels in 2022. Considering a milk consumption per wheel of 600 lt, at an average price of 0,6675 €/lt, a total of € 5.822.963 on average is locked in aging every year by each one of the 295 producers. This monetary value only considers the milk's cost, not considering all other costs. If additional costs like labor, energy and any other production related costs, that value would be higher, giving a higher immobilized capital. For the sake of the explanation and to be more conservative in the data analysis, only the cost of the milk will be considered.

Given the availability of data, the assumption that aging lasts up to 30 months will be made. This gives a further conservative scenario, given that the stock won't be valued for cheese aged more than 30 months, meaning that the most valuable wheels will be neglected, leading to a lower than actual value for the total stocked value.

Looking at 2022 stock data (Table 4) (available on the official Parmigiano Reggiano consortium website up to October 2022), it is possible to evaluate the average stock value that each producer has immobilized in its warehouse and an estimation of the stock composition will be made.

The tables below show the total stock, the stock of wheels with less than 18 months (18-) of aging and with more than 18 months (18+) of aging. The stock level is fairly constant with very low fluctuations around the average value of 2.066.899 wheels. Given that there are 295 producers, their average total stock is 7.006,4 wheels, of which around 65% are wheels aged less than 18 months, 35% are aged more than 18 months.

	TOTAL STOCK	STOCK 18-	18-/TOT	STOCK 18+	18+/TOT
MONTH/YEAR	**2022**	**2022**		**2022**	
January	2.037.578	1.321.994	65%	715.584	35%
February	2.041.810	1.309.256	64%	732.554	36%
March	2.042.317	1.327.584	65%	714.733	35%
April	2.051.271	1.345.281	66%	705.990	34%
May	2.057.013	1.382.514	67%	674.499	33%
June	2.075.667	1.415.361	68%	660.306	32%
July	2.098.479	1.401.421	67%	697.058	33%
August	2.076.482	1.358.211	65%	718.271	35%
September	2.102.631	1.352.093	64%	750.538	36%
October	2.085.747	1.332.726	64%	753.021	36%
AVERAGE	2.066.899,50	1.354.644,10		712.255,40	
PER PRODUCER AVERAGE	7.006,40	4.592,00		2.414,40	

Table 5. Warehouse composition and valuation

Since the data analyzes total stock, stock of 18- wheels and greater 18+ wheels, the assumption that only 4 kinds of aging exist was made: 12, 18, 24 and 30 months aging.

Looking at 18- aged wheels, the stock was valued in the following way:

- $^1/_4$ of the total 18- stock valued at production cost of 10,0125 EUR/kg. This proportion was chosen in order to make the "youngest" wheels' average stock amount, equal to 1148 wheels per month, roughly match the average monthly production, equal to 1130 wheels produced per month.

$$\boldsymbol{Production\ cost = \frac{0{,}6675\ EUR/lt * 600\ lt/wheel}{40kg/wheel} = 10{,}0125\ EUR/KG}$$

- $^2/_4$ of the total 18- stock valued at 2022 average 12 months aging wholesale price = 10,73 EUR/kg

- $^1/_4$ of the total 18- stock valued at 2022 average 18 months aging wholesale price = 11,15 EUR/kg

Considering now the 18+ wheels stock, it was evaluated in the following way:

- $^1/_2$ of the total 18+ stock valued at 2022 average 24 months aging wholesale price = 11,98 EUR/kg
- $^1/_2$ of the total 18+ stock valued at 2022 average 30 months aging wholesale price = 12,7 EUR/kg

STOCK 18- VALUATION [EUR]	
Less than 12 months of aging	459.775,39 €
12 months of aging	985.446,18 €
18 months of aging	512.009,55 €
TOTAL 18-	1.957.231,12 €
STOCK 18+ VALUATION [EUR]	
24 months aging	578.496,25 €
30 months aging	613.263,97 €
TOTAL 18+	1.191.760,22 €
TOTAL	3.148.991,34 €

Table 6. Warehouse evaluation based on wholesale prices

Following the assumption that was made on the proportions of different aged wheels within a producer's warehouse, a total locked amount of 3.148.991,35 € is obtained. This value is the maximum stock the average producer could potentially tokenize. Given that for this solution an overcollateralization is required, the producer won't be allowed to tokenize its whole warehouse,

although it will be able to put its whole stock as collateral. The maximum amount the producer will be able to tokenize depends on the over collateralization proportion: for this specific solution, a 25% of over collateralization (on top of the actually tokenized warehouse value) seemed a good compromise that would both enhance the producers' incentives to respect the tokenization conditions and the investor would feel protected from this level of overcollateralization. Looking at numbers, a 25% over-collateralization means that the maximum amount the producers can tokenize is 80% of its whole stock, which would in turn lead to having the whole 100% of the stock set as collateral, which the producer would be legally obliged to use to pay back investors in case it was not able to meet its obligations.

This way of evaluating the warehouse is not a sound and valid accounting evaluation, since stock in the balance sheet is recorded at production cost, but it is a market evaluation that is needed in order to understand how much the producer can profit from its stock, how much it could tokenize, how much it would receive from investors and how much it will have to pay as interest.

6.5. INTEREST PAYMENTS

The token will be designed in order for it to behave and be managed similarly to a security. This means that the producer will have to pay periodic interest payments to the investors, up to maturity date, where the payment will consist of the last interest payment and the reimbursement of the price paid at token issuance.

Investors that want to buy the token at issuance date, will have to pay the token issue price decided by the producer, which will be determined as:

$$\boldsymbol{Price = \frac{Tokenized\ Warehouse\ Value}{Number\ of\ Tokens\ Issued}}$$

Given that the producer is tokenizing part of its warehouse, the interest paid to the investors will be closely linked to the aging process, so that the tokens "age" too, until they reach maturity. For this reason, it was decided to give the token holders part of the increase in value (wholesale price) of a cheese wheel during its aging process. This means that if a wheel has a 10% increase in value when going from one aging period to another, the investors will be given a portion of that increase.

In Table 6 it's possible to view the evolution in value (measured in EUR/KG) of Parmigiano Reggiano and the difference and percent increase in value every 6 months (starting from month

12) of aging up to a total of 30 months of aging. As previously stated, the newly added cheese wheels are valued at their raw material cost (milk). From 0 to 12 months of aging, it was decided not to evaluate the increase in value for the two following reasons:

- 6 months aged wheels aren't sold on the market, so it's difficult to give them a market value.
- It gives the producers a 12 month "grace period" on the interest payments, so that the producer can initially fully focus on deploying the capital in the most efficient way, without having to focus on paying back interest payments 6 months after the token issuance.

This means that interest payments will start on month 12.

AGEING [MONTHS]	0	12	18	24	30
WHOLESALE PRICE [EUR/KG]	10,013	10,73	11,15	11,98	12,7
PRICE DIFFERENCE [EUR/KG]		0,718	0,42	0,83	0,72
% VALUE INCREASE		7,17%	3,91%	7,44%	6,01%

Table 7. Parmigiano Reggiano's wholesale prices analysis

The producer, based on its choice, will decide what proportion of that "% value increase" to allocate as payments to investors, and what percentage of that rent will retain for itself. In order to be attractive to the market and to save on costs in proportion to the raised amount (given that the interest rates are fixed at issuance and based on Parmigiano Reggiano's price at that time), the producer will have to give to investors a share between ⅓ and ¼ of the value increase. All the shares of the value increase dedicated to the investors will then be summed up in order to constitute the 6 months interest rate. After that calculation is made, the interest payments will be planned as such:

- at the 12 month mark, the investors will receive double the interest rate, which will simply be the double of the 6 months interest rate.
- starting from the 18th month mark, the investors will receive the 6 month interest payment

The investors in this way will receive payments that mimic very closely the actual warehouse value increase, since every 6 months the different aged wheels gain value.

If instead of wholesale prices the retail prices were used for the analysis, the producer would have a higher value of the stock leading to a potentially higher tokenizable value, but would have to pay a higher amount of interest, given that retail prices are higher than wholesale prices as shown below.

AGEING [MONTHS]	0	12	18	24	30
RETAIL PRICE [EUR/KG]	10,013	15,16	16,75	17,38	19,3
PRICE DIFFERENCE [EUR/KG]		5,1475	1,59	0,63	1,92
% VALUE INCREASE		51,41%	10,49%	3,76%	11,05%

Table 8. Parmigiano Reggiano's retail prices analysis

After this analysis, the producer and its choices come into play: How attractive does he want to be to investors? How much liquidity does it need? What is its risk attitude? It will have to compare the token it will issue with any other competing financial instrument available at the moment.

Given that this tokenization solution is most likely to be adopted by SMEs (Small Medium Enterprises), it can be compared to a similar traditional financial instrument: minibonds. The producer will have to compete with this traditional financial instrument in order to be the most attractive offering on the market.

6.6. Minibonds [31]

Minibonds are defined as “debt securities (bonds and commercial papers) issued by non-financial companies, for an amount lower than € 50 million.”

Minibonds were first created in 2012 to help SMEs to find and exploit new sources of funding. Ever since, the minibond industry has been growing, in both number of issuers and issued amounts. All the data that will be shown, refers to the timeframe from 2012 to 2021.

Since minibonds were born in 2012, they have been used to raise a total of € 8,07 billion, of which € 2,85 billion were raised by SMEs.

In 2021, 219 minibond issues were monitored: the total raised capital was € 1.068 billion, the average emission size was € 5 million, of which 67% raised less than € 5 million and 38% raised less than € 2 million.

The charts below show the evolution of minibond emissions, where the proportion of lowest ranges of capital raised increased at the detriment of the higher ranges of raised capital: in 2021 77% of the emissions raised less than € 5 million and 43% raised less than € 2 million. This reinforces the idea that minibonds and alternative financing forms are the most appreciated for those businesses that don’t need to raise large amounts of capital, so Parmigiano Reggiano producers could be put in this group of SMEs looking for ways to raise “small” liquidity amounts without having to appeal to traditional capital raising instruments. Given the warehouse evaluation above, the average Parmigiano Reggiano producer would fall in the range of companies that emit the lowest value minibonds.

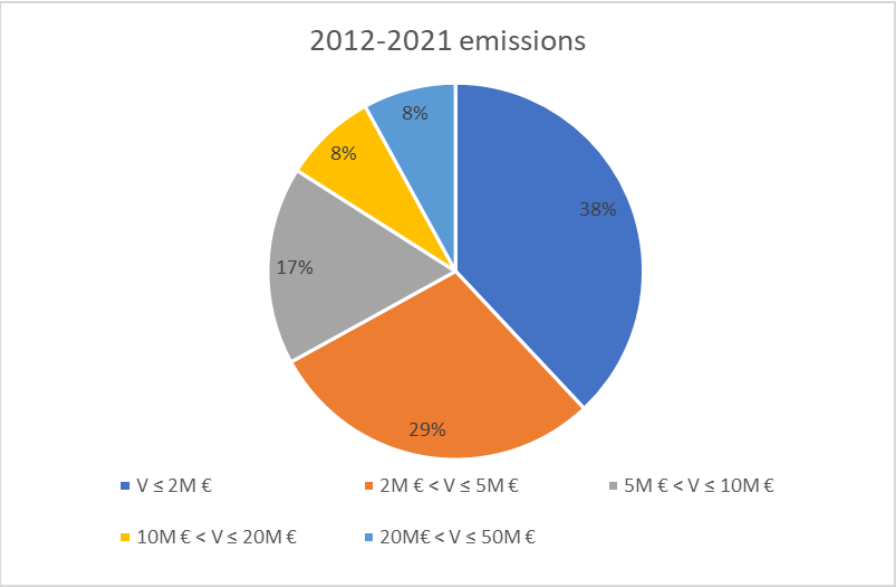

Figure 21. 2012 - 2021 minibond emission sizes

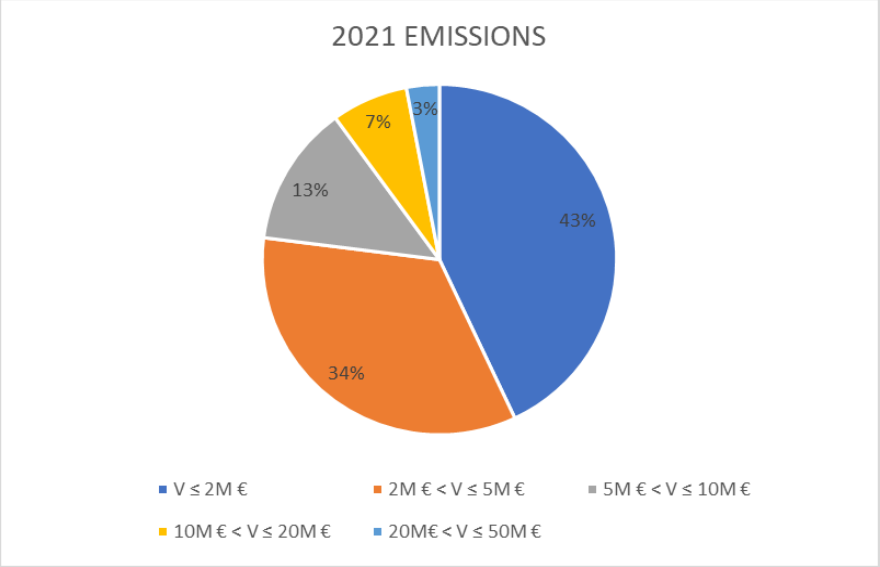

Figure 22. 2021 minibod emission sizes

The average maturity of a minibond emitted in 2021 is equal to 5,63 years. Looking at the whole considered time period (2012-2021), the average fixed annual coupon is equal to 4.38%, with a median value of 4,25%. Concentrating now on the issues made by SMEs (which account for 63,7% of the whole 2021 issues) with maturity dates between 2 to 3 years, the average coupon was 5,5%. So the Parmigiano Reggiano producer will have to compete with this interest rate, given that the tokens' life span would be of 30 months, which is equal to 2,5 years.

Minibonds have the possibility to be rated by specialized rating agencies, that after reviewing the companies' accounts, give a rating on based on the capability of the issuer to meet its interest

obligations. Among the whole sample, only 29% of the total minibonds were rated, whereas in 2021 that percentage increases to 34%. This is evidence of the fact that emitting companies want to reassure investors that they will be able to pay the coupons and payback the face value at maturity.

Moreover, the emitting enterprises can choose to put a collateral as a protection for the investors. The case in which directly the issuer set its own assets as a guarantee occurred in 15% of the emissions of 2021. Among all the other issuers, 31% had their emission guaranteed by the Fondo di Garanzia, 15% were covered by SACE (Sezione speciale per l'Assicurazione del Credito all'Esportazione) whose aim is to help those companies that want to expand internationally and 13% had guarantees from the Regions.

6.6.1. Requirements to issue traditional minibonds

The requirements for unlisted SMEs to emit a minibond are the following:

- Have fewer than 50 employees and an annual turnover or an annual balance sheet of less than € 10 million (So-called Small Enterprises) or fewer than 250 employees and an annual turnover of less than € 50 million or total balance sheet assets of less than 43 million euros (so-called medium-sized enterprises);
- Have published their last two financial statements, the last of which certified by an auditing firm;
- They are not banks or micro-enterprises, i.e. companies with fewer than 10 employees and an annual turnover or balance sheet of less than 2 million euros.

If the issuer (the enterprise that will get the funds and manages all corporate actions) and the subscriber (qualified or institutional investors) have opted for the listing of the security on the Extra Mot market of Borsa Italiana (that is the secondary market for minibonds), the issuer must fulfill the following obligations:

- Drafting of the admission prospectus, that contains the terms and conditions, so the amount issued, the nature of the minibonds, rights and duties of the involved parties,
- Request for the ISIN code from the Bank of Italy, that is a code that uniquely identifies a security,
- Publication of the last two financial statements, of which the last one is audited;

- Application for the admission of the minibonds to be traded on the Extra Mot segment of Borsa Italiana, that is the section reserved to bonds,
- Publication of the Prospectus or Admission Document at least 3 days before the date envisaged for admission to trading.

Following the admission of the minibonds to trading, the issuing company will be required, in order to be compliant with the Extra Mot Regulation of Borsa Italiana, to publish the following information:

- the annual financial statements subjected to audit, without delay and in any case no later than six months after the end of the financial year to which they refer,
- any information related to the issuer that may have a positive or negative effect on the price of the minibonds,
- any change in the characteristics of the issue or in the procedures for exercising the rights of the holders of the minibonds,
- any changes in rating judgments, if they were previously made public,
- technical information about the minibonds, like information on the calculation of interest and any early repayment of the securities.

The actors involved in a minibond issuance and the costs business has to bear to emit a minibond are the following:

- Advisor: is a consultant that partners the enterprise in the initial strategic decision, in drafting the business plan and in defining timing and the means of the emission. Advisors cost between 0,5% and 2% of the raised capital. The average 1,25% will be used for the analysis.
- Legal consultants/Law firms: make sure that the process is in compliance with the existing law and regulamentation, and control the accuracy in the adopted procedures and the correct execution of contractual rights and duties. Law firms usually cost between € 12.000 and € 22.0000. The average € 17.000 will be used for the analysis. Assuming legal consultants will usually also do the financial statements' certification, which has an average cost of € 10.000 per year, so a total cost of € 30.000 will be considered.

- Arranger: deals with the placement of the securities on the market and finding potential investors. Arrangers cost between 0,5% and 1,5% of the raised capital. The average 1% will be used for the analysis
- Rating companies: gives a financial rating on the solvency capability of the emitting company. Rating costs between € 5.000 and € 15.000 for a SME and the cost reduces by 40% in the following years. This is an optional cost since the emitting business can decide whether to get rated or not. Given the 30 months duration (which is equal to 3 years) the total average cost is € 22.000
- Depository and agent bank: often are the same institution (a bank) and it has a cost of € 5000 per year, so a total cost of € 15.000 will be considered.
- Marketing agency: can be used in order to publicize the issuance among investors

An additional cost is represented by the choice of giving centralized management of the securities to an authorized authority like Monte Titoli in Italy, that then proceeds to the security dematerialization. Dematerialization is the process for which the physical securities certificates (the pieces of paper) are removed from circulation and replaced by their electronic version. This facilitated transactions, making them faster and safer than with on-paper recorder transactions. This feature is embedded within the blockchain, where there is no need for a central authority to facilitate circulation, investors can just buy and sell the token how they prefer in an easy, fast, secure and transparent manner. The cost for this feature in traditional minibonds emission is € 4500 for three years duration. This cost will be considered in the total emission cost, since ease of circulation is embedded within blockchain technology.

Regarding the investors base, in 2021, Italian banks underwrote 43% of the minibonds volume, followed by private debt funds for the 23%, foreign funds and banks for the 14% and then the Cassa Depositi e Prestiti (which is a joint stock company owned by the Italian State 83% and some banks (17%)) for the 9%.

6.7. Tokenization vs minibonds

As stated above, minibonds are a relatively new financial instrument used to raise liquidity and their employment has been increasing since 2012. Warehouse tokenization could be a valid competitor and alternative to minibonds for one main reason: less actors involved in the process leading to lower transaction costs, faster emission and potentially more attractiveness towards investors.

Thanks to issuance through blockchain technology, producers will be able to reduce total emission costs, this would in yutn lead to being able to either offer the same interest payments to investors at a lower cost than the traditional instrument or could offer higher interests at the same cost of the traditional minibonds.

Having less actors involved in the whole process also leads to lower information asymmetry between the emittent and those actors involved in helping the emission process, which in turn leads to faster and cheaper emissions. Moreover, the producer will be able to fully understand the process and will be in full control of the emission.

For this use-case the producer will be forced to over-collateralize the tokens with 125% of the raised capital, giving investors a higher level of protection than in traditional minibonds. In case of insolvency, the producer will be legally obliged to use the collateral to raise liquidity in order to pay back investors.

6.8. Tokenization process - STO

The process of issuing a security token on the blockchain and selling it on the primary market is called Security Token Offering (STO).

Once the producer decides to tokenize its warehouse, it will have to contact a blockchain company that will guide it in the process, unless it has a blockchain developer among its workforce. The assumption made in this case is that the issuer has no blockchain hard skills or blockchain employee, so it will have to rely on an external company, expert in asset tokenization.

6.8.1. Token compliance

The blockchain company will have to make sure to make the whole tokenization and maintenance processes compliant to the current Italian regulation on security tokens.

The updated version of the MiFID II (Markets in Financial Instruments Directive) (Directive 2014/65/EU) that came out in 2014, gives the same definition of securities as the Italian law, so security tokens aren’t explicitly included in such definition. However, recently the Italian authority for securities (CONSOB), stated that the tokenization process is very close to that of creating traditional securities, for this reason “investment tokens” and “security-like tokens” qualify as securities.

Since the tokens are considered just like securities for a juridic point of view, their emission must follow the regulation established by the Italian legal system that deals with bonds, which consists of articles of the civil code from 2410 to 2420-ter. Those articles regulate the issuance of bonds by joint-stock companies. Joint-stock companies however, are not the only companies that can issue bonds: to these are added the Limited Partnership by Shares and the LLCs (Limited Liability Companies). This means that as of now, an enterprise that decides to issue security tokens will have to respect all the obligations required for traditional securities issuance.

6.8.2. Requirements

For this reason, security tokens must contain the following information in order for the emission to be compliant:

- the name, object and company's registered office, with the indication of the Company Register office where the company is registered. This is provided straight away by the producer
- the share capital and reserves existing at the time of issue. This means that the producer will need to have its balance sheet approved.
- the date of the issuance and of its entry in the register.
- the total amount of the issue, the nominal value of each security, the rights attributed to them, the yield or the criteria for its determination and the method of payment and repayment, any subordination of the rights of the bondholders to those of other company creditors. The issued amount will be the value of the tokenized percentage of the warehouse, the nominal value (face value) is the primary market price, the rights are stated in the contract (and they will be substantially to have the right to dispose as one prefers of the token and to receive the interest payments)
- any guarantees by which they are assisted. In this particular case the guarantee is the overcollateralization, equal to 125% of the emitted amount.
- the date of repayment of the loan and the details of any prospectus. In our example the loan will be repaid after 30 months and the producer should post a prospectus on what it intends to do with the raised capital

Since the producer/issuer will need to have its balance sheet audited in order to redact a balance sheet, the warehouse stock (in numbers and value) will be evaluated too. This warehouse audit is

fundamental for the producer in order to understand how much it can possibly tokenize and how much the collateralization would be. If the warehouse stock wasn't audited and approved, it could lead to a potential stock over evaluation, that could lead to potential insolvency of the issuer. In case of an undervaluation of the warehouse, the producer wouldn't be efficiently raising capital, leading to the possibility of not seeing any value in creating such a financial instrument.

A third trusted party will have to approve the balance sheets. This goes against the decentralization and trustlessness concept of the blockchain, but there is no viable alternative to it, since it is the only way to contrast the "garbage in, garbage out" principle. [32]

6.8.3. The smart contract

The token standard that is usually employed for security tokens is the ERC1400, firstly developed by Polymath. This standard allows the producer to have full control over the tokens. When Polymath developed this token standard, some essential functionalities were decided (these bullet points are taken directly from Polymath's founder Github post):

- "must have a standard interface to query if a transfer would be successful and return a reason for failure.
- must be able to perform forced transfer for legal action or fund recovery.
- must emit standard events for issuance and redemption.
- must be able to attach metadata to a subset of a token holder's balance such as special shareholder rights or data for transfer restrictions.
- must be able to modify metadata at time of transfer based on off-chain data, on-chain data and the parameters of the transfer.
- must support querying and subscribing to updates on any relevant documentation for the security.
- may require signed data to be passed into a transfer transaction in order to validate it on-chain."

All of these points were decided upon so that the issuer can "protect" investors in case drastic solutions are required (for example in order to revert fraudulent transactions) and to make the issuance compliant.

To implement all these functionalities, the ERC1400 tokens bundle together different standards (a standard is a recognized state of the art of a token) [33]:

ERC-1594: **Core Security Token Standard**

Given the requirements investors have to satisfy (KYC and AML, whitelisted wallet), transfers of securities may fail for different reasons. This doesn't occur in utility tokens where usually, if there are transfer fails, the reason is an insufficient balance.

ERC-1410: **Partially Fungible Tokens**

When tokenizing an asset, many tokens are created. These tokens must be different from one another, but are related to the same underlying asset. So these token will be partially fungible. By adding metadata to the tokens, it's possible to make these tokens non-fungible with fungible traits. For example it's possible to separate token issued during the primary offering from those that were acquired on the secondary market.

Creating separations will allow the issuer to better manage all the tokens.

ERC-1643: Document Management Standard

Security tokens usually have documentation attached. In this case it would be information about the offering, price, maximum supply, maturity date, interest payments and all the requirements listed above. Moreover, the financial statements could be attached to the tokens, for an additional level of disclosure and transaparency

ERC-1644: Controller Token Operation Standard

Given that security tokens are considered as securities, they will be subject to regulations and legal oversight, based on the jurisdiction and regulatory framework they are deployed in. For this reason it may occur that the issuer has to force transfer the tokens from one wallet to another. This may occur in the event of having to reverse fraudulent transactions or help investors in the event of the loss of their wallet's private keys.

These tokens are EVM compatible, so they can be implemented on any blockchain that uses an EVM, like Ethereum and Polygon. Given all the discussion that was made before on Layer 2 scaling solutions, releasing the token on Polygon (an Ethereum's Layer 2 solution that uses plasma chains)

would be a good solution: given its high level of security with scalability properties, Polygon is being adopted more and more from both users and on-chain startups, leading to a potential high level of adoption, leading to a large potential investor base.

By providing all the issuance information stated above to the blockchain company, the smart contract will then be written and deployed on the blockchain. As an example, the main parameters are:

- Token supply is 100.000 tokens,
- The tokenized warehoue's value is 3.000.000, so each token will cost € 30.
- The interest payments rate, that is decided looking at the average wholesale prices available. In case the producer doesn't want to use the average prices, it could provide the invoices of its sales, so that each producer could have its own dedicated rates, but this would lead to a higher emission cost because the legistimacy of the invoives would need to be checked,
- Maturity date on which the last payment is done and all the supply burnt,
- Only investors whose wallet is in the whitelist will be able to mint the token, so only investors that have passed the KYC (Know Your Customer) and AML (Anti-Money Laundering) will be able to either buy the token during the primary offering or on the secondary market,
- The roles of each actor involved with the token issuance and maintenance, which will be the following: investor, that will receive the payment and the issuer, which will be the actor (the producer or a delegate) in charge of managing the toke throughout its lifecycle.

6.8.4. Primary offering

Once the seecurity token issuance is approved by the CONSOB and registered, the primary offering is organized. The primary offering is the process for which the tokens are sold and released in the market. Given that the blockchain company, by creating these smart contracts, offers a digital financial service, in accordance with the Legislative Decree 231/2007 and subsequent amendments, potential investors will have to go through a KYC and AML process. KYC and AML are basically a set of questions the aim of which is to prevent illegal activities such as money laundering, fraud, and financing of terrorism by ensuring that organizations know who their

customers are and that they are not dealing with individuals or entities that are involved in illegal activities. All those investors that will want to become token holders will have to pass those checks, otherwise the token may be seen as non compliant. This means that the wallet of those investors that were successfully whitelisted will have their wallet enabled to mint (buy) that token during the primary offering, or that their wallets will be able to hold that token if they buy it on the secondary market. If the wallet is not whitelisted, given the checks that are embedded in the ERC1400 token, it won't be able to be a holder, and the transactions will be blocked.

TOnceday of the primary offering arrives, the producer puts all the tokens on sale at the decided price and interested investors buy the tokens. The producer could even perhaps add a function in the smart contract where, if a certain capital threshold isn't reached, the funds are given back to the investors (just like it happens in fundraising).

For the solution that was developed, investors will be required to buy their security tokens with a EURO pegged stablecoin: as of now, the most reliable is EUROC, developed by Circle. Circle deposits € 1 every time 1 new EUROC, this means that each token is backed by the same amount in FIAT currency. This kind of cryptocurrency is designed to have the same value as a FIAT EURO meaning that in any moment in time, 1 EUROC= € 1. This is a requirement for the investors in order to facilitate the producers' funds management: since Italian law requires a tax to be paid on any capital gains generated above € 2000 (as of 2023 Italian's budget law), it would be a burden for the producer to have to pay capital gain taxes. EUROC can be bought on most of the exchanges and can be easily converted from other tokens on the most used wallets.

From now on, the assumption that the whole token supply has been sold to investors will be made.

The STO can be considered closed at this point. From now on, the issuer will have to manage the tokens' lifecycle, until maturity date, 30 months after.

6.8.5. Token lifecycle

At this point, if the blockchain company has developed its own marketplace where all the tokens it helps to issue are listed, the warehouse tokens will be listed on it, creating a secondary market. If instead the blockchain company doesn't have a proprietary marketplace, the producer will either have to look for one that allows the listing of ERC1400 tokens, since most of the marketplaces allow for listing of only ERC721 and ERC1155 tokens. The producer will most likely decide to be

assisted by a company that has its own marketplace, since it will make sure that all the potenital investors go through the KYC and AML checks. This is fundamental otherwise the token may be seen as non compliant.

Finding a marketplace to list the token will help the producer to get to be known among investors and, if the producer is able to meet all payments and to provide clear information, in the future it might be able to issue a higher amount of tokens and have a larger potential investor base.

The producer will issue security tokens with a defined maturity. When maturity date is reached, after 30 months in our example, the producer will pay the last interest payment plus the face vale reimbursment. Once all the payments have been successfully sent out and received, the whole supply is burnt. This means that the whole token supply is automatically sent to a burn address. A burn address is a wallet address to which nobody has access to the private key. An example of burn address is 0x000000000000000000000000000000000000dEaD. Once the tokens are sent there, the token can't be retrieved in any way. This is the equivalent of destroying the token, but since tokens are created from smart contracts and once a contract is deployed on the blockchain it can't be removed, the only solution in order to destroy a token is to send it in a location to which no one has access to.

6.9. Warehouse auditing

Since this security is tokenizing an asset, meaning that it is backed by a valued asset, the issuer has to make sure that the asset doesn't lose value, otherwise the collateralization may fail the token will lose all its value, and investors might start a legal action against the issuer for neglicenge in the asset management.

The way the issuer will ensure that the warehouse is still valuable, at least as much as the collateralization established by the security, it has to have the warehouse audited every year by an empowered third party. This auditing may fall within the yearly balance sheet auditing that is required, so the enterprise will not have to sustain other costs outside those sustianed for the redaction of the balance sheet.

At this point, after the wheels are counted and evaluated at their wholesale price, the producer will post the document, showing how much the warehouse is worth from a market point of view and if the collateralization is still at 125% of the emission value.

With fluctuating Parmigiano Reggiano prices, the value of the warehouse may change and the collateralization percentage might change too: if the price per wheel increases, the percentage of the warehouse that is put as collateral decreases, given that each wheel will be worth more, so there will be less wheels at stake as collateral to be used in case the producer wasn't able to cover its obligations. This is the optimistic scenario, but what happens if the warehouse value decreases? Two potential scenarios must be evaluated at this point:

- the producer tokenized less than 80% of its warehouse, leading to a total overcollateralization of less than the whole warehouse
- the producer tokenized 80% of its warehouse, leading to having the whole warehouse put as collateral

6.9.1. Lower than 80% tokenization

If the producer tokenized less than 80% of its warehouse, meaning he didn't have to put 100% of its warehouse as collateral, the producer will only have to make sure to have enough wheels to correctly collateralize the securities. Let's make an example: consider a warehouse whose value is of 100 wheels * 10 €/wheel = € 1000, the producer tokenizes 60% of the warehouse, meaning it will issue tokens for a total of € 600, the total collateralization is equal to 1,25% of the issue value, so € 750, which corresponds to 75 wheels, always assuming the same average value of 10 €/wheel. t0 is the issuance date, t1 is the time in which the warehouse value is established. If the average price of the wheels drop to € 9, the producer will have to make sure to have enogh wheels to re-establish the correct collateralization value. In the table below, it's possible to appreciate how the variation in price with respect to the variation of wheels set as collateral aren't proportional.

	t0	t1	VARIATION
AVERAGE WHEEL PRICE [EURO/WHEEL]	10	9	-10,0%
ISSUANCE [EURO]	600	600	
COLLATERAL [EURO]	750	750	
COLLATERAL [WHEELS]	75	83,3	11,1%

Table 9. Collateralization scenario analysis

6.9.2. 80% warehouse tokenization

In this case the producer will have to pay to the investors the difference between the total emission value and the collateral: if the producer raised a total of € 10 million by tokenizing 80% of the warehouse, the total collateral will be equal to € 10 million + € 2,5 million of over collateralization. This means that at the issuance date, the whole warehouse (100%) is worth € € 12,5 million. Assuming the price of cheese makes the warehouse's value drop down to € 11 million (so a 12% drop in value), the emission wouldn't be correctly collateralized. For this reason, the producer will be required to pay out the difference between the total emission value and the value that reinstates the correct collateralization proportions. By doing some proportions, since the new 100% value of the warehouse is € 11 million, the 80% of that would be € 8,8 million. Hence the producer will have to pay 10-8,8= € 1,2 million to the investors. In this way the new emission total will be equal to € 8,8 million, with a 125% collateralization worth € 11 million. This mechanism is a protection for both investors, that are holding a security that is always correctly collateralized, and issuers, that in this way are sure to be able to cover their obligations in case they become insolvent and stop paying the interest payments and final face value payment.

This process would be applicable in case the price decreases by a large enough threshold that allows price fluctuations, otherwise the producer would have to continuously adjust the collateralization, making it very expensive and inefficient. This threshold could be set at a -2,5% variation in price. If that threshold is reached and surpassed, that the dynamics explanied above would come into play. This value was taken by looking at the prices posted on CLAL.it website.

6.10. Interest payments

As previously stated, the producer will have to pay interest to the investors every 6 months, up to month 30, starting after 12 months from token issuance.

For the same reasons stated above, the payments will have to be made in EURO pegged stablecoins like EUROC. This makes it easier for the producer to directly convert FIAT currency in cryptocurrency, easily understanding the amount of cryptocurrencies it has to buy, with a very low probability of fluctuations, leading to the devaluation of the token.

In the smart contract, each spot interest rate will have to be stated before issuance. The amount is decided at the beginning with the current wholesale prices of different aged wheels and giving a share of the increase of value that occurs from one period to the following to the investors.

In order to make the payments, the smart contract will be programmed in the following way: the producer can lock a given period's interest payment amount in the smart contract starting from 5 days prior to the actual paying date. The payments then go out proportionally to each investors' token holdings on the due date. This takes the transactional burden off of the producer. In this way the producer is fully in control of the amount that is being sent out to the investors and doesn't have to rely on a third party (calculating agents or transfer agents). On top of this, having a lead time between the payment and the deposit is a protection for the producer in case it has issue with the conversion from FIAT to crypto currency. The smart contract and the tokenization platform will inform it whether the correct amount was uploaded on the contract or not. On the 30th month, the producer will have to upload on the contract that period's interest rate plus the face value (price) that investors paid to buy the token.

After the payment has been successfully received by each investor, the token will burn itself in the way explained in the Token lifecycle chapter.

6.11. Token's market valuation

As any other security that is listed on an exchange, the market will give a price to the token. In this specific case, the token's price will be closely linked to Parmigiano Reggiano's wholesale price. The relationship between tokens and Parmigiano price is the same inverse proportionality that is present between bonds and interest rates: if Parmigiano's wholesale prices drop, the token price will increase and vice versa. This would occur because, if cheese prices increase, the producer will have to offer higher interest rates, so the tokens that were issued before would lose value becasue they offer lower interest rates linked to previous lower cheese prices.

From this point of view, the producer would obvisously hope for the prices to always increase, making it easier for it to pay back the interest and not risk to have a lower collateralization, since € 1 of the warehouse at the time of issuance would be worth more than that if wholesale prices increase. As the issuer pays the interest payments, investors will gain trust in the producer. This trust will most likely propagate outside to other potential investors, creating a supply shock, leading to an increase in the token's price.

6.12. Emission economics: Traditional vs On-chain emission

Is it really convenient for a producer to go through all the trouble of a token issuance on-chain with respect to a traditional minibond emission?

In order to make such a comparison, a traditional and on-chain emission of the same size will be considered: the average producer will tokenize its warehouse, which in this case is the average warehouse value calculate before, worth € 3.148.991. For all the reasons explained above, the emission will be 80% of the warehouse's value, meaning that the emission will be worth € 2.519.193,12.

Regarding the difference in emission and maintenance, costs are the following:

COSTS FOR TRADITIONAL EMISSION

COST	**AMOUNT**
ADVISOR (1,25% of the emission)	31.489,9 €
ARRANGER (1,0% of the emission)	25.191,9 €
LAW FIRM	17.000,0 €
RATING	22.000,0 €
FINANCIAL STATEMENTS CERTIFICATION (3 years)	30.000,0 €
DEMATERIALIZATION AND CENTRALIZATION OF SECURITIES	4.500,0 €
DEPOSITORY AND AGENT BANK (3 years)	15.000,0 €
TOTAL	145.181,8 €

Table 10. Traditional emission costs

COSTS FOR ON-CHAIN EMISSION

COST	AMOUNT
ADVISOR (1,25% of the emission)	31.489,9 €
ARRANGER (1,0% of the emission)	25.191,9 €
LAW FIRM	17.000,0 €
RATING	22.000,0 €
FINANCIAL STATEMENTS CERTIFICATION (3 years)	30.000,0 €
TOTAL	125.681,8 €

Table 11. Blockchain emission costs

Considering the on-chain emission, the costs regarding "DEMATERIALIZATION AND CENTRALIZATION OF SECURITIES" and "DEPOSITORY AND AGENT BANK" were dropped, given that they won't be costs the producer would have to pay. Not only this, but half the cost for the arranger was considered, given that the blockchain would take away some of its work. The total emission and maintenance costs are lower for an on-chain, however the cost for the tokenization wasn't considered. Given that the blockchain developer company knows the advantage the producer has in issuing by collaborating with them, logically it will make a price such that the total costs are still lower than in case of a traditional emission.

Then the interest payments must be considered. In the case of a traditional emission, as stated before, the average 5,5% yearly coupon payment for 2-3 year maturity minibonds will be considered. Regarding the On-chain interest payments, the sum of the allocated percentage of value increase will be used as interest payments (Int6). The interest payments start at month 12, with double the interest rate, and then are paid every 6 months up to maturity. In order to make a correct comparison, since the maturity date is 30 months after the issuance, which is equal to 2,5 years, the last "traditional" payments will be equal to half the yearly payment, so on month 30, investors would receive the payment based on a 2,5% interest rate. Below a timeline that compares the two emission types.

TRADITIONAL ISSUE INTEREST RATE			5,5%		5,5%	2,75%
TIME (months)	**0**	**6**	**12**	**18**	**24**	**30**
ONCHAIN ISSUE INTEREST RATES			2 x Int6	Int6	Int6	Int6

Table 12. Interest rates comparison

For the overall analysis, 4 main variables weretaken into account:

- Interest rates
- Tokenized percentage of warehouse
- Total cost
- Percentage of cheese value increase

First, the analysis was carried out by fixing the Blockchain based solution's interest rate equal to the traditional interest rate (equal to 5,5%). Three scenarios of warehouse tokenization were analyzed, taking into consideration the cases the producer tokenizes 80% (equal to a € 2519193,1 emission), 65% (equal to a € 2.046.844,4 emission) or 50% (equal to a € 1.574.495,7 emission) of its warehouse. These three tokenization percentages were analyzed because they are those that give a raised capital can be

In this case it's possible to notice that blockchain emissions cost less than traditional emissions. This means that the capital that investors provide to the issuer will be allocated and invested more efficiently and gives a higher degree of protection to the investors.

	TOKENIZED % OF WAREHOUSE	80%	65%	50%
INTEREST RATE 5,5%	**% OF CHEESE VALUE INCREASE TO INVESTORS**	26%	21%	16%
		TOTAL COST	**TOTAL COST**	**TOTAL COST**
TRADITIONAL		491.570,89 €	415.995,10 €	340.419,31 €
BLOCKCHAIN		459.474,93 €	386.260,88 €	313046,83
DIFFERENCE		32.095,96 €	29.734,22 €	27.372,48 €

Table 13. Scenario analysis with fixed interest rate

The second analysis was done by making the cost of the traditional emission equal to the one of a blockchain emission and comparing the resulting interest rates, it's clear how, in compliance with the previous analysis, the producer can either offer the same interest rates at a lower total cost, or offer a higher interest rate to investors at the same cost of a traditional emission.

SAME TOTAL COSTS	**TOKENIZED % OF WAREHOUSE**	80%	65%	50%
	% OF CHEESE VALUE INCREASE TO INVESTORS	28%	23%	18%
		RATE	**RATE**	**RATE**
TRADITIONAL		5,50%	5,50%	5,50%
BLOCKCHAIN		6,01%	6,08%	6,20%
COST		491.570,89 €	415.995,10 €	340.419,31 €
DIFFERENCE		0,51%	0,58%	0,70%

Table 14. Scenario analysis with fixed and euqla total costs

This means that if blockchain emissions start being adopted from more and more enterprises, those that want to issue their minibonds in a traditional way will most likely have difficulties in finding investors for two main reasons:

- warehouse tokenization can offer higher returns,
- the higher returns come at a lower cost for the issuer, meaning that it will be able to fulfill more easily its obligations than in a traditional emission, making the investor feel more protected

6.13. Current state of art of token securities and emissions

In Italy, there has not been a specific regulation for security issued on a DLT. This means that, as stated above, a security token issuance must follow the same exact process and compliance of traditional securities.

In practical terms, this leads to the fact that today, issuing a security token, means creating a digital twin of a regular security. The issuer won't benefit from the use of the blockchain if it were to issue today because of the following reasons:

- the regulation is the same as for traditional security tokens, meaning that the actors involved are the same in a traditional issuance
- it is not possible to make the interest payments on blockchain. When the interest payments due dates come, the issuer will send the correct amount of money, in FIAT currency, through a regular wire transfer.
- it is not possible to issue tokens only with the smart contract, the traditional "paper" contract will have to be redacted in compliance with regulation. When investors buy a token, it will sign the smart contract with its wallet and will also sign the regular contract that gives all the information about the issuance and interest payments.

As long as the Italian Government doesn't regulate token securities, this will be the way of issuing tokens.

In Luxembourg instead, in 2019 the Bill no.7363 was passed and it states that "Account-keeper may hold securities accounts and register securities in securities accounts within or through secure electronic registration devices, including distributed electronic registers or databases. Successive transfers recorded in such a secure electronic registration device are considered like transfers between securities accounts. The holding of securities accounts within such a device secure

electronic registration or registration of securities in securities accounts through such a secure electronic recording device does not affect the fungible nature of the securities concerned."

This gives tokens the same legal status like the one that is given to traditional securities. [34]

In France, thanks to the 2019-486 bill of May 22 2019 (also known as "PACTE law"), a clear and defined regulation for initial offerings for Utility tokens only. The law explicitly excludes security tokens from the regulation, but having the government starting to regulate the use of DLTs is a good starting point, rather than having no regulation at all. [35]

7. CONCLUSIONS

Given the current state of art in Italy regarding tokenization, is there any benefit for the issuer and the blockchain solution developers? At the moment the total cost of emission is basically equal to that one of a traditional emission, but as a first mover in this field, the issuer would have various benefits:

- it would receive more attention and assistance from the company that would enable the blockchain issuance since few companies are experimenting in this field
- being a first mover would lead to gaining experience and the DOs and DON'Ts linked to such a solution, whereas those that issue for the first time would have to learn the good practices at their expenses

From the point of view of the blockchain solution developers, they would too gain experience on what the issuers' necessities are and how to make the whole process more efficient for both them and the issuers, leading to a better customer experience in both terms of cost and solution and reducing the costs for the development of the solution.

Looking at blockchain in more general terms, once its use will become more user friendly, more and more people will try operating on it, that could in turn lead to an exponential adoption of blockchain based solutions. As of now, in order to be able to use a blockchain, the user should have at least an idea of how the technology works in order not to be scammed and to make the transactions secure. The same thing happened for internet: those that used internet first were those that saw value and wanted to learn how to use it and the processes that went on in the background. As time passed, internet became much easier to use and the preliminary education wasn't needed anymore, leading to higher adoption

One thing is certain, many big names for various industries have been investing heavily in experimenting with this new technology. The groundbreaking application is yet to be found, but once that will happen, this technology adoption will increase drastically.

BIBLIOGRAPHY

[1] https://www.studocu.com/en-us/document/massachusetts-institute-of-technology/blockchain-and-money/241-a-brief-history-of-ledgers-before-starting-my-investigation-into-by-llfourn-unraveling-the-ouroboros-medium/17178823

[2] https://corporatefinanceinstitute.com/resources/knowledge/accounting/double-entry/

[3] https://www.wallstreetmojo.com/general-ledger/

[4] https://medium.com/nakamo-to/whats-the-difference-between-decentralized-and-distributed-1b8de5e7f5a4#:~:text=In%20a%20centralized%20system%2C%20control,refers%20to%20differences%20of%20location

[5] https://hedera.com/learning/distributed-ledger-technologies/what-are-distributed-ledger-technologies-dlts

[6] https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html#:~:text=Structure%20of%20a%20Block&text=The%20block%20is%20made%20of,contains%20more%20than%20500%20transactions

[7] https://www.coindesk.com/learn/bitcoin-halving-explained/

[8] https://nitk.acm.org/blog/2021/10/01/prisoners-dilemma-and-its-influence-on-blockchain-consensus-models/

[9] https://xorbin.com/tools/sha256-hash-calculator

[10] https://andersbrownworth.com/blockchain/blockchain.

[11]https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[12] https://www.ledger.com/academy/blockchain/web-3-the-three-blockchain-generations

[13] https://towardsdatascience.com/blockchains-versus-traditional-databases-e496d8584dc

[14] https://www.ledger.com/academy/what-is-the-blockchain-trilemma

[15] https://learn.bybit.com/blockchain/fastest-cryptocurrencies-high-tps/

[16] https://ethereum.org/en/layer-2/

[17] https://medium.com/techskill-brew/layer-2-blockchain-scaling-solutions-channels-sidechains-rollups-and-plasma-part-16-79819e058ef6

[18] https://bitcoinminingcouncil.com/bitcoin-mining-electricity-mix-increased-to-59-5-sustainable-in-q2-2022/

[19] https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume).

[20] https://digiconomist.net/bitcoin-energy-consumption

[21] https://digiconomist.net/ethereum-energy-consumption

[22] https://www.galaxy.com/research/whitepapers/on-bitcoins-energy-consumption/#:~:text=At%20the%20time%20of%20writing,113.89%20TWh%2Fyr%20in%20total.

[23] https://www.nasdaq.com/articles/research%3A-bitcoin-consumes-less-than-half-the-energy-of-the-banking-or-gold-industries

[24] https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html

[25] https://101blockchains.com/cryptocurrency-legal-countries-list/

[26] https://www.internetworldstats.com/emarketing.htm

[27] https://www-statista-com.ezproxy.biblio.polito.it/statistics/1202503/global-cryptocurrency-user-base/

[28] https://www-statista-com.ezproxy.biblio.polito.it/statistics/730876/cryptocurrency-maket-value/

[29] https://consensys.net/blockchain-use-cases/digital-identity/

[30] https://www.clal.it/index.php?section=parmigiano_parma#1214_n

[31] 8° REPORT ITALIANO SUI MINIBOND, “Dipartimento di Ingegneria Gestionale, Politecnico di Milano, 2022”

[32] https://www.soldionline.it/guide/prodotti-finanziari/la-disciplina-dei-corporate-bond

[33] https://medium.com/@bitcademyfb/security-token-standard-erc-1400-tokenization-of-assets-f92ba6ee6b85

[34] https://www.coindesk.com/markets/2019/02/15/luxembourg-passes-bill-to-give-blockchain-securities-legal-status/

[35] https://www.pwc.lu/en/blockchain-and-crypto-assets/luxembourgs-bill-blockchain-held-securities.html