



Cattedra

---

RELATORE

---

CORRELATORE

---

CANDIDATO

Anno Accademico

## SUMMARY

Blockchain technology may not yet be at a critical mass, but I am certain that it will be, and that any organization, particularly those in the banking and financial services industries, that does not begin experimenting with this revolutionary technology now will be forced to recover in the future.

**Blockchain is an innovative technology that allows untrusted people to share data in a decentralized network.** While it may be used as a simple database file to protect data and documents, Blockchain technology has the potential to **create completely autonomous businesses where all software and goods run through smart contracts performed on the Blockchain.** As a result, enterprises must comprehend the potential of Blockchain technology in order to plan their Blockchain strategy.

This technology can be thought of as an **application layer that runs on top of the existing stack of internet protocols.** This means that it adds an entirely new layer to the internet to allow for economic transactions (Swan, 2015). Using Blockchain technology, Bitcoin users can exchange their digital cryptocurrency through a decentralized system that allows for digital integrity, reliability, transparency, and immutability, as well as levels of openness that were previously unheard of. All the benefits listed above are enabled by the foundations upon which the technology is built, in **this work these are outlined and described from a functional stand-point with just the required technical knowledge to clearly understand why elements like cryptography enable security and trust, but without the ambition to argue against or support specific technical foundation of the technology, these are described to show the reader how the frequently cited benefits of transparency, immutability, trust and decentralization are enabled.**

The technology in this work is analyzed from a business point of view, since my daily work is to consult companies about their Blockchain adoption strategy, I wanted to analyze and report what the technology can actually do for businesses. **Therefore, the main enablers of Blockchain technology are presented,** and they are: Tokenization, Notarization and Smart Contracts. Nowadays, everyone appears to be fascinated by the prospect of incorporating blockchain technology into their current business model or utilizing blockchain technology to solve existing problems. **Blockchain, on the other hand, cannot be used in every situation.** Businesses must conduct a thorough analysis of their current business problems before implementing this new and promising technology.

Below is illustrated a high-level framework, made up by three main steps, that can help companies analyse weather they could benefit from the adoption of Blockchain technology.

Step 1: Identify the ecosystem the company is in. This means have a clear idea of all the stakeholders involved in the core business processes.

Step 2: Analyse whether there's the need for a trusted framework to be adopted. If there is no need for trust between parties, or parties already trust each other completely, then Blockchain would lose its added value; therefore, more traditional automation systems would suit better.

Step 3: Once it has been understood that the company would benefit from the use of blockchain, it is time to understand which are the benefits that the company is actually looking for.

- Smart contract: they can help companies automate their processes by adopting a "if/then" approach tailored to the specific use case by implementing specific rules into them.

- Tokenization: tokenized assets can be exchanged throughout the value chain and carry information that can be updated in each step of it. The tokenization of assets is used in traceability solutions, where, through the use of Non-Fungible Tokens (NFT) products can be tokenized and carry with them the whole production processes related information.

- Notarization, among the three, is the one that affects the least existing processes, yet bringing an incredible value to ecosystems composed of different stakeholders that need their interactions to be trusted.

**Once established what Blockchain can do for businesses the major roadblock is whether to use a public Blockchain or a private one or opt for a mix of the two and adopt a hybrid Blockchain solution.** Since I believe this affects significantly many aspects of the potential adoption of Blockchain by businesses, the main differences, pros and cons of the three have been outlined. Briefly, public blockchains represent all the principles upon which the technology is built and enable true trustless interactions and decentralization. Public blockchains are also the most commonly known (e.g. Bitcoin, Ethereum) and I personally believe that are the only ones that enable the users to extract the most value out of their adoption. On the other hand, being all the transactions public and access permissionless, these may not be always the best choice for companies willing to adopt it into their processes. Therefore, to understand what are the key needs and what is the value that a business wants to extract from this technology is fundamental in this choice, but simply private blockchains can bring more benefits for B2B, or at least same benefits than public ones but with less drawbacks, while public blockchains can be thought more as a solution for B2C and B2B2C processes.

**The second chapter of my thesis is focused on analysing the different trends or applications within the Blockchain space that I had the opportunity to study the most, being for passion and curiosity or for work.** Going by order, the first one is **Decentralized Finance (DeFi)**, a movement

that aims at making a new financial system that is open to everyone and does not require trusting intermediaries like banks. To achieve this DeFi relies heavily on cryptography, blockchain and smart contracts. Decentralized Finance is a very young trend that experienced an extremely high growth over the past two years, to give a reader a grasp of such growth it is possible to use the Total Value Locked (TVL) metric, or, the value of all the assets (mainly cryptocurrencies) that are deposited into DeFi protocol, or, applications that enable users to use specific services like lend, borrow, bond, etc. Indeed, the TVL has gone from ~\$600mln in January 2020 to ~\$230bln in January 2022<sup>1</sup>. With the aim to give the reader the understanding of all the main opportunity within the DeFi space, **I have tried to go through the most used services such as lending & borrowing and liquidity providing entering into the details of what are mechanics and formulas that major protocols use such as the constant product market maker**. Moreover, as I have personally found myself lost among the extremely high returns that are promoted on many protocols, **I have tried to go through the many risks that DeFi has, such as:**

- **Smart contract risk**, or the risk of the code upon which all the mechanics are thought to work being purposely or unconsciously wrote with errors.
- **Volatility**: naturally all cryptocurrencies are very volatile, therefore returns paid in the form of cryptocurrencies may be substantially lower, in terms of dollars, once the user effectively earns them.
- **Impermanent loss**: the risk that users incur when providing liquidity to a given protocol and have their assets grow in value, this growth may not be fully captured if the asset was locked into a liquidity pool paired with another asset which price is not or negatively correlated with.

The second application analysed is **Blockchain Traceability**. Consumers, business partners and regulators are increasingly demanding transparency and organizations struggle to provide the data due to the lack of connectivity between the networks of the supply chain. This leads to highly manual efforts and reconciliation activities which are often outsourced and exposes data to third parties. Moreover, it is increasingly strategic to improve tracking and visibility of qualitative and sustainable activities and parameters.

**Blockchain can help organizations to transform so they can give consumers, business partners and regulators the transparency they demand in ways that create lasting business value.** Blockchain Traceability solutions provides a trusted platform for traceability and transparency within

---

<sup>1</sup> <https://www.statista.com/statistics/1237821/defi-market-size-value-crypto-locked-usd/>

an ecosystem through the use of notarization and tokenization. **This technology can help businesses deliver long-term value by improving brand equity, sustainability and revenues.**

In my thesis are analysed three different use cases of business that have adopted the technology to their supply chain, namely Blockchain Wine Pte. Ltd. (with the platform TATTOO Wine), Carrefour and ANSA, these are just a small portion of the business adopting the technology to improve their processes and deliver higher transparency to their consumers.

Even as the enthusiasm around the usage of blockchain-based traceability has grown, it is critical to remember that many of these applications are still in their infancy. **I believe that my work provides a thorough understanding of the technological foundations of blockchain traceability, additionally, a summary of the many uses of blockchain traceability in various areas is outlined, with a focus on the solutions that EY has developed in this field for different clients.** For the sake of completeness, the use case of ANSA is reported here as well. The Agenzia Nazionale Stampa Associata (ANSA) has developed, in collaboration with EY a solution for the verification of the provenance of a given news. ANSA was facing a challenge of trust due to the high number of third parties copying its news and altering them for many reasons, as for instance increase click-through rates, conversion rates etc.

Therefore, ANSA developed ANSAcheck, ANSAcheck is a **news certification system powered by blockchain technology that ANSA has chosen to tighten control over the flow of its news, ensuring that they cannot be used or disseminated in an untruthful or inappropriate manner,** while also guaranteeing readers the source's highest quality and reliability.

By using the “stamp” at the end of an ANSA news item or "ANSA source," it will be able to:

1. Verify the history and credibility of a news item by referring to the main source.
2. Allow for comparisons between the news read and the ANSA source.
3. By improving public trust, enable editors, agencies, and media to qualify as quality news producers.

**On a technical level the solution consists of four main steps:**

1. When the news is created by ANSA, the Blockchain records its identifier so that its future events can be tracked and an hash of the content of the news is created.
2. When the news is modified or updated by ANSA, the Blockchain records the event allowing transparent versioning.
3. When the news is resumed by the Publishers participating in the initiative, the Blockchain verifies the authenticity of the news recorded by ANSA and records the resumption event

enabling future consultations of the news resumed by the publisher thanks to the ANSAcheck stamp.

4. When the end-users want to verify the reliability of the news they can click on the ANSAcheck button on the end of the page, see the hash of the news as well as the notarisation transaction happened on the Blockchain.

A further analysis of this Blockchain use case finds **3 main benefits for ANSA to have adopted such solution:**

1. Enable ANSA and its main clients to establish themselves as a quality supplier by fostering public trust.
1. Bridge the divide between journalism and the publishing ecosystem's participants.
2. Develop new business logics and models (reputation system, as-a-Service replicable solution, etc.).

The initiative's objective was to provide an innovative solution for the traceability of news in the publishing and journalism industries via the use of blockchain technology and its inherent properties of immutability, transparency, and security. **The purpose of this project is to follow the tale of ANSA-published news that is disseminated to its clients or is reported by other parties (agencies, news outlets) with attribution to the ANSA source.** The suggested approach sought to distinguish ANSA news from those of other news suppliers. By using blockchain to monitor the news narrative, ANSA could solidify its brand and publications may join a trustworthy ecosystem and profit from its reputation. ANSA will therefore preserve his trusted brand by preventing it from being associated with false news and will also be able to track the quantity of news articles reposted by other providers. ANSA is therefore the world's first news organization to establish a true public Blockchain-based news management system.

**The third application that I decided to include in my work is relative to the accounting and auditing,** Blockchain technology is one of the most disruptive new technologies in auditing and accounting; while the development and research of blockchain applications by audit companies remain in their infancy, they may one day increase the audit's quality, efficiency, and efficacy. Integration of accounting on blockchain reveals the potential for streamlining unnecessary operations, increasing transaction settlement speed, and preventing financial report fraud. Additionally, it will be capable of influencing corporate governance procedures. **A concrete example of a use case applied to the accounting is the triple entry bookkeeping, or an additional public layer added to the existing double entry system where companies add data which is notarized on the Blockchain and publicly visible to all the stakeholders,** potentially reducing transactional and settlement costs (never was I meant to say that this would make audits activities no longer needed). **Follows the**

**example used in my thesis the explain this use case.** Take into account a buying products transaction in which company B (buyer) purchases an item from company S (seller), who will generate an invoice at the time of purchase. In a double entry system, this results in the need to perform two series of pair and opposite book entries. Company B will first create bookings for the buying and the subsequent creation of debt; subsequent to payment, the buyer will create bookings for a movement that will eliminate the debt and result in a cash flow to the supplier. Company S, on the other hand, will need to make its own bookings, first for the release of the sale item from the company in exchange for the creation of a credit with the buyer, and then for a financial movement associated with the elimination of the credit-related item and the emergence of cash-in-flow. By implementing a triple entry model on a blockchain, it would be feasible to increase the system's efficacy and efficiency. **Among the network's many participants, the triple entry system would produce a unique shared ledger in which all transactional information would be stored.** A single public ledger enables automatic updating via a single book entry and enables communication and availability to all counterparts. Assume the identical financial transaction mentioned above between the two companies, this time, each actor will have two distinct entries, one pertaining to the acquisition/sale of the item and another pertaining to the payment. Company S would produce and sign a transaction comprising the purchase data at the moment of sale to company B. **When signed by both parties, the event will be put in the distributed ledger, where it may be audited.** The buyer would be obligated to pay the seller an amount in exchange for the commodity X upon inscription in the public ledger. **The smart contract would control the relationship between the two parties by temporarily rendering the funds specified by the purchaser ineligible for use as security by the debtor.** At the moment of delivery, the smart contract would release and transfer the cash to the seller, rendering the debt uncollectible. Information is encrypted and subsequently rendered immutable in this system, making it difficult to forge or erase registered information.

**The last application I chose to report and explain is the digital identity,** being very actively involved in the Self Sovereign Identity world since I currently collaborate for the development of one of the seven use cases proposed by the European Blockchain Service Infrastructure (EBSI), a collaborative effort of the European Commission and the European Bank for Reconstruction and Development. **The objective of EBSI is to use blockchain to speed the development of cross-border services for public administrations and their ecosystems in order to validate data and increase the trustworthiness of services.** EBSI has been developing a network of dispersed nodes around Europe since 2020, enabling applications focused on certain use cases. EBSI is the first pan-European blockchain infrastructure, built on open standards and a transparent governance approach. **Self-sovereign identity, abbreviated SSI, is a new paradigm for digital identification on the**

**internet**, i.e., how we develop trusted connections with websites, services, and applications with whom we need to establish trusted relationships in order to access or secure private information. SSI is a paradigm change in digital identity, driven by new technologies and standards in encryption, distributed networks, cloud computing, and smartphones. **Rather of leveraging blockchain technology to create and send/receive bitcoin, identity management leverages it to create a decentralized public key infrastructure (DPKI).** In essence, blockchain as well as other decentralized network technologies can provide a robust, decentralized solution for exchanging public keys directly between peers to establish private, secure connections and recording some of these public keys on public blockchains to prove the signatures on digital identity credentials (verifiable credentials) **that peers can exchange to establish proof of real-world identity.**

All in all, why is self sovereign identity (SSI) so important? Because it represents a shift in the locus of control, putting the citizen/user at the centre of it by decentralizing the structure. The locus of control in centralized and federated identity models is with the network's issuers and verifiers. **The focus of control changes to the individual user in the decentralized SSI identity paradigm, who may now engage with everyone else as a complete peer.**

**Finally, in the third and last chapter of this dissertation I focused on the application of blockchain to securitization.** Since 2017, token offers have been gaining traction as a means of acquiring funds for businesses and digital securitizations of physical and financial assets is expected to expand reaching up to 70\$ billion in financing by 2026, up from the capitalization of about \$3 billion in 2020<sup>2</sup>. **Tokenization eliminates entry barriers, allowing any asset investable for a global investor base and provides a number of advantages that fundamentally enhance asset holders' and investors' market access.** Along with lowering total issuance costs, tokenization enhances asset accessibility and attractiveness. Specifically: it eliminates the need for an intermediary, reducing costs and time; saving critical time and money; assets with large minimum ticket amounts may be fractionated with no additional fees and with an all-digital infrastructure, asset ownership may be transferred instantly and globally; lastly, its time to market is reduced by standardizing and automating the issuance and management processes. Nevertheless, tokenization has also several related issues. Those regarding SME stocks are due to the fact that most SME stocks are unlisted, bond issuance is not provided and there are limited options beyond loans. With reference to real estate, for instance, there is high demand but low liquidity as well as large tranches and large

---

<sup>2</sup> [https://www.azimut-group.com/documents/20195/1674564/CS\\_AzimutToken\\_230321\\_ENG\\_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a](https://www.azimut-group.com/documents/20195/1674564/CS_AzimutToken_230321_ENG_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a)



notes. On the other hand, unbankable and illiquid assets can be accessed only by insiders and in many cases cannot be transferred or their transferability is limited.

In the last paragraphs of the third chapter I have **described the main existing blockchain-based securitization platforms that can be found on the market**, such as Azimut, Wizkey Define, Hypermasts, Securitize and Stonize and their securitization process. **Basically, the securitization process involves two flows: the sales flow and the purchase flow.** In the first one the asset is placed on the market in the form of a token with a rating provided by the platform used. This flow foresees the possibility for sellers to update the information available regarding the positions offered. During the creation phase, the seller decides whether to list a portfolio of assets or a single asset, entering the necessary data in a document containing the relevant information of the position. Then, the platform performs an initial check to assess the completeness of the data quality and assigns a rating (rating phase). In this way the seller has access to the simulation area of the pricing tool where he can calculate the value of his assets using parametric mathematical models. Once the seller is satisfied with the data quality, the tokenization process begins and the representative security tokens is created directly on the platform. Afterwards, sellers can send accredited investors to the platform, manage all data allowing investors to operate and trade on the platform. Position information can be updated and transactions can be approved via transfer agent functions also on the secondary market. In order to ensure compliance during issuance/transfer, the figure of the on-chain Transfer Agent is envisaged. In particular, the Transfer agent can carry out digital onboarding and token assignment, the transfer of authority to another centralized figure and can have control the securities offering. When Security tokens are issued, they are only assigned to eligible and approved investors. Finally, vendors are able to execute KYC online process, on-chain investor whitelisting and direct communication with the approved investor. In the purchase flow the user/entity, after being identified and approved by the platform, purchases the asset in the form of a token and has the possibility to monitor it over time via the platform. After being invited by the issuers, the potential buyer performs the KYC directly through the platform, so that they can analyze the data uploaded to the platform and view the general information of the positions (access phase). Only after being approved, the investor is whitelisted, the blockchain address is verified and the user/entity can check all the PDF documents associated with the positions and perform their own evaluations (approval phase). After choosing the investment, the investor executes the bank transfer and receives the security token, which incorporates all relevant information and effectively represents the investment made (purchase phase). In the end the investor can monitor the lifecycle of the position, updated by the seller and has the possibility to approve all.



Cattedra

---

RELATORE

---

CORRELATORE

---

CANDIDATO

Anno Accademico



# TABLE OF CONTENTS

TABLE OF FIGURES.....	3
INTRODUCTION.....	4
CHAPTER I - BLOCKCHAIN TECHNOLOGY.....	6
1.1. Principles of blockchain .....	6
1.2. Cryptography .....	7
1.2.1 Hash .....	8
1.2.2. Blocks.....	9
1.3. Key system and digital signatures.....	10
1.4. Wallet .....	11
1.5. Consensus mechanism.....	12
1.5.1. Proof of Work (PoW).....	12
1.5.2. Proof of Stake (PoS) .....	13
1.6. Blockchain enablers .....	14
1.6.1. Notarization.....	14
1.6.2. Tokenization.....	15
1.6.3. Smart Contracts .....	18
1.7 Blockchain typologies .....	20
1.7.1. Public blockchain.....	20
1.7.2. Private blockchain.....	21
1.7.3. Hybrid blockchain.....	22
1.7.1. Bitcoin Blockchain .....	22
1.7.2. Ethereum Blockchain.....	23
1.8.3. Ripple Blockchain.....	25
CHAPTER II – BLOCKCHAIN APPLICATIONS.....	27
2.1 Decentralized Finance (DeFi) .....	27
2.1.1 Lending and Borrowing.....	28
2.1.2 Liquidity Pools.....	32

2.1.3	Constant product market maker and Impermanent Loss .....	34
2.2	Traceability .....	36
2.2.1	Food & Beverage .....	37
2.2.2	News & journals.....	43
2.3	Auditing and Accounting.....	48
2.3.1	Triple entry accounting.....	50
2.4	Digital identity .....	51
2.4.1	European Blockchain Service Infrastructure (EBSI) and European Self Sovereign Identity Framework (ESSIF).....	56
2.5	Results of the survey .....	58
CHAPTER III - BLOCKCHAIN APPLIED TO THE SECURITIZATION .....		62
3.1.	Introduction to securitization through blockchain .....	62
3.2.	Benchmark: existing blockchain based securitization platforms on the market.....	63
3.2.1.	Azimut.....	63
3.2.2.	Wizkey Define .....	64
3.2.3	Hypermasts .....	67
3.2.4	Securitize .....	68
3.2.5.	Stonize .....	70
3.3.	AS-IS: Securitization of credits using the Blockchain .....	72
3.4.1.	Smart contract services .....	73
CONCLUSION .....		77
BIBLIOGRAPHY .....		79
SITOGRAPHY.....		80

## TABLE OF FIGURES

Figure 1 - Hashing of data .....	9
Figure 2 - Creation and validation of blocks.....	10
Figure 3 - Immutability of data .....	10
Figure 4 - Monthly NFT volumes in USD on Opensea.....	17
Figure 5 - Decision making process to adopt Blockchain .....	20
Figure 6 - Losses to liquidity providers due to price variation compared to holding the original funds supplied.....	36
Figure 7- SWOT analysis of Carrefour traceability solution .....	42
Figure 8 - ANSAcheck button.....	45
Figure 9 - Info about News ID and News Hash .....	46
Figure 10 - Visualization of the transaction on the Blockchain.....	47
Figure 11 - Triple entry book-keeping model.....	51
Figure 12 - Relationship between us and organization under the account-based identity model of the internet .....	52
Figure 13 - Social login buttons .....	53
Figure 14 - The shift from centralized/federated identity model to Self Sovereign Identity.....	55
Figure 15 - Self Sovereign Identity Framework.....	56
Figure 16 - Creation of the token by the seller.....	74
Figure 17 - Purchase of the token by the buyer .....	75
Figure 18 - Update of information and additional payments .....	76

# INTRODUCTION

A latest innovation is sweeping the world, one that began with a new marginal economy on the web and an alternative end-to-end digital currency called "Bitcoin" which was issued and backed by an automated consensus among networked users via algorithmic self-policing transactions over the internet in a decentralized trust-less public ledger system, rather than by a central authority.

Blockchain is the term used to refer to this ledger. While Bitcoin is establishing itself as a trustless digital money, the underlying Blockchain technology is gradually demonstrating its far greater significance. While the world has not yet reached the critical threshold for adoption of Blockchain technology, it is widely believed that this revolutionary technology is here to stay and that any company, that has not begun experimenting with it may find itself late and in need to recover.

Firstly, this dissertation takes an attempt to give the reader the needed understanding of Blockchain on a technological level, indeed, in order to understand what is the potential of this disruptive technology a basic understanding of how it works under the hood is needed. Moreover, the content of this work is aimed at give to everyone willing to adopt Blockchain a framework to understand what is the value it can bring and wether it is suitable for the specific use case, basing the analysis on metrics and KPIs.

Moreover, this work aims at give visibility to the use cases already in place for this technology in different sectors, from supply chain traceability to financial services, I believe that having a condensed overview of all of these different application would inspire readers and give them the tools to understand Blockchain value proposition and to understand the technology beyond the widely known application in the cryptocurrency space.

Finally, a deeper analysis has been done on the financial services sector, outlining the main concepts of Decentralised Finance, the existing solutions for the securitization of assets using tokens and smart contracts and proposing a solution that builds upon the latters to tackle some of the issues that businesses face in the adoption of Blockchain technology for the securitization using tokens.

Most of the content in this work comes from my last year experience in EY Advisory where i had the opportunity to study in deep Blockchain and its applications for companies, having participated in most of the use cases that are discussed in Chapter 2. Therefore, the sources of this work come mainly from meetings with professionals from different sectors, colleagues, on-hand experience and books.

Personally, I come from a management background, thus one year ago the only knowledge I had about Blockchain came out of articles and books that for my personal curiosity I was studying. This led to the research for a job position within the space and to find it at EY as a Blockchain Business Advisor. To everyone approaching this topic I would like to convey the message that as complicated as it could seem at first glance,

the expertise in this fast-growing field is still under development and the learning curve is very steep, therefore compared to many other sectors the time spent to learn about Blockchain would yield a much higher level of expertise when compared to other more established fields.



# CHAPTER I - BLOCKCHAIN TECHNOLOGY

Essentially, Blockchain is a technology and in its original form, it is a distributed database technology that builds on a tamper-proof list of timestamped transaction records and its innovative power stems from allowing parties to transact with others they do not trust over a computer network in which nobody is trusted and that trust mechanism is enabled by a combination of peer-to-peer network of computer nodes, consensus-making, cryptographic hashing mechanisms, and market dynamics.<sup>1</sup>

Stuart Haber and W. Scott Stornetta initially proposed blockchain technology in 1991<sup>2</sup> as a way to construct a system in which document time stamps could not be altered with. However, it was over two decades later, in January 2009, with the debut of Bitcoin, that blockchain saw its first real-world use. Blockchain is widely acknowledged to be based on the four basic pillars relating to the principles of encryption, consensus, decentralisation and ownership:

1. Distributed computation
2. Public key encryption
3. Consensus decentralised
4. Blockchain possession

Since the late 1980s, there have been studies on an effectively interlacing of the first two pillars in several ways in order to establish a virtual monetary environment, the most significant one in the 1990s by D. Chaum's Digicash<sup>3</sup>. On the other hand, in Adam Back's Hash cash<sup>4</sup>, published in 1997, decentralized agreement was originally used as a DDoS countermeasure. Finally, the tight interweaving of the three pillars gave light to the blockchain mechanism we now know.

This combination was initially studied in the research writings of Nick Szabo<sup>5</sup> and was then further studied in Satoshi Nakamoto's Bitcoin whitepaper, the first blockchain paper ever to be published.

## 1.1. Principles of blockchain

**Distributed computation:** usually, Blockchain is a shared public ledger. In the widest meaning of the word, distributed computing indicates that numerous systems share processing power, which may also be located in various places. In general, every participating user is needed to download a full copy of the blockchain, which includes all of the protocol's history up to that point. In the Bitcoin blockchain for instance each participant

---

<sup>1</sup> Mendling et al, 2018

<sup>2</sup> Haber, S., Stornetta, W.S. How to time-stamp a digital document. J. Cryptology 3, 99–111 (1991)

<sup>3</sup> D. Chaum, "Untraceable Electronic Cash", Goldwasser S. (eds) Advances in Cryptology — CRYPTO' 4 88, 1990.

<sup>4</sup> A. Back, "Hashcash - a denial of service counter- measure", 2002.

<sup>5</sup> N. Szabo, "The Bitgold proposal", 2005.

must download all transactions that have been registered in the blockchain in order to access the network. After this stage, every node may run independently, analyse and propagate each incoming transaction: all nodes will automatically synchronize the recorded transactions – hence, central node processing and distribution of the data are not necessary. In addition, every node can help to achieve consensus.

**Public Key encryption**, also known as asymmetric cryptography, is a cryptography technique that uses two mathematically linked numbers: the first, known as the private key, and the second, known as the public key, which is generated from the former by the use of a complicated mathematical function. Each one has a distinct purpose. The public key is used to encrypt, while the private key is used to decrypt: these two keys combined form a user's digital signature. Calculating the private key from the public key is computationally impossible. As a result, public keys may be widely distributed, providing users with a quick and convenient way for encrypting material and validating digital signatures while still protecting users' privacy.

**Consensus decentralised:** as previously stated, blockchain is essentially a network-distributed repository in which nodes constantly record information in "blocks" that are built into a specific "chain." To establish decentralized consensus, one party no longer has to go via a central authority or trust the other party in order to communicate data.

During these years, several consensus methods have been established. Considering the non-technical nature of this work though, the thorough treatment of distributed consensus methods is confined to the most popular use cases, namely Proof of Work (PoW) Proof of Stake (PoS) and Proof of Authority, which will be discussed further on in this chapter.

## 1.2. Cryptography

It is now critical to get a thorough understanding of cryptography before proceeding with a thorough explanation of blockchain cryptography. What is cryptography? In the most strict sense, crypto refers to secrets. As a result, cryptography technologies seek to provide full or pseudo-anonymity<sup>6</sup>. The major uses of cryptography focus on assuring the security of participants and transactions, protections against double-spending, and the absence of control of central authority on activities. Cryptography has a wide range of applications. It can help in some situations to secure various network transactions.

On the other side, it has applications in the verification of the exchange and sharing of tokens and assets. Blockchain applications use cryptographic techniques and private keys to simulate the idea of real-world signatures. Cryptography techniques perform use of complex mathematical codes to store and transmit data

---

<sup>6</sup> R.C. Merkle, "Protocols for public key ecosystem"

values in secure ways. Consequently, it assures that only the people meant as the recipient for the transaction or data transfer may receive, view, and handle the same, as well as verify the validity of the participants and the transaction itself.

Essentially, cryptography is a mechanism for securely transmitting information between two or more parties. Before delivering a message to the recipient, the sender uses a certain type of key and algorithm to encrypt it. The recipient then uses decryption methods to get the original message. Hence, what is the most essential component of cryptographic operations? The solution is clearly encryption keys.

Thanks to encryption keys, unauthorized recipients or readers are unable to read a message, a number, or a transaction. They are excellent options for ensuring that only the intended receivers may read and handle a given message, data item, or transaction. As a result, keys can impart 'crypto' characteristics to data.

The bulk of blockchain applications, particularly on public blockchains, do not rely on the need to send private, encrypted messages. A younger generation of blockchain apps, indeed, use several kinds of cryptographic encryption to ensure the security and total anonymity of transaction information. Many new tools with various functions linked to cryptography applications in blockchain have evolved throughout the years. Hashing and digital signatures are two prominent instances of the above-mentioned tools

### 1.2.1 Hash

A hashing algorithm is a mathematical function that reduces input information to a predetermined size. The outcome of the computation is known as a hash or a hash value. Hashes are used to identify, compare, and execute calculations on files and data strings. Typically, the software computes a hash before comparing the data from the original documents.

A simple example of hashing is digitally signing software and making it available for download. In order to do this, it is needed a hash of the script of the application to download. It is also needed a hashed digital signature. When the data set is hashed, the software is encrypted, and it may then be downloaded. As a result, when anyone downloads the software, the browser must decrypt the file and compare the two distinct hash values. The browser then executes the same hash function, employing the same method, and hashes both the file and the signature once more. If the browser correctly generates the identical hash value, it may validate that the signature and the file are both legitimate and have not suffered any change.

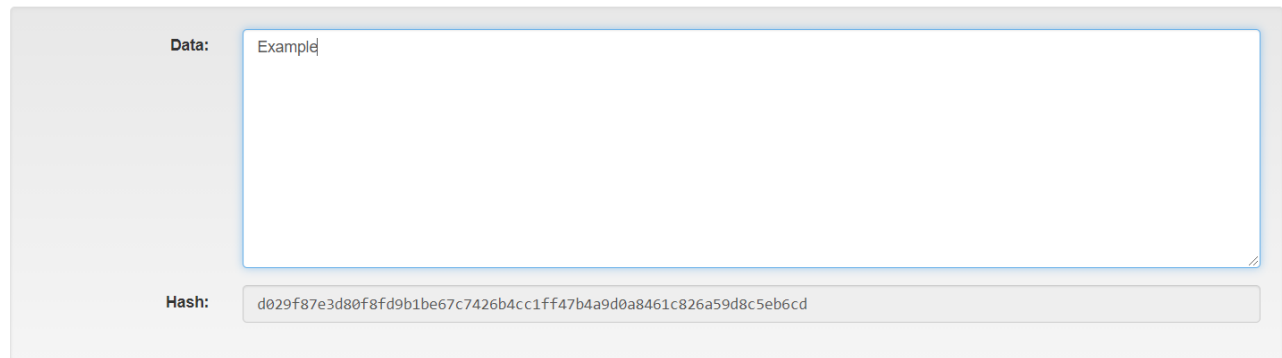
The most adopted hash function in Blockchain is the SHA256<sup>7</sup>, below there is an example of the creation of a hash from a random data input ("example")

---

<sup>7</sup> <https://en.bitcoinwiki.org/wiki/SHA-256>

*Figure 1 - Hashing of data<sup>8</sup>*

## SHA256 Hash



Data:	Example
Hash:	d029f87e3d80f8fd9b1be67c7426b4cc1ff47b4a9d0a8461c826a59d8c5eb6cd

Hash values are predictable and responsive to the parameters of the algorithm's supplied variables. The same series cannot be replicated using an alternative information source as input, hence why hashing is so helpful for cryptocurrencies. The resulting hash of data entered is both unique and irreversible. For instance, an input of "123" will always result in the same output. If this were not the case, and 123 produced a different result each time it was hashed, the procedure would lack consistency and validity. This means that your programs will never communicate in the same language.

### 1.2.2. Blocks

Blocks are used to store sequences of valid transactions that have been hashed and put into a Merkle tree<sup>9</sup>. Each block contains the hash of the previous block on the blockchain, which connects the two. A chain is formed by the connected blocks. This recursive procedure validates the preceding block's integrity all the way down to the first block, known as the genesis block.

Separate blocks can be generated concurrently, resulting in a temporary fork<sup>10</sup>. Aside from a secure hash-based history, every blockchain contains a predefined method for scoring multiple versions of the past so that the one with the highest score may be chosen above others.

In the figure below there is an example of a series of block. It is possible to note that each block has a field "data" that is where information is recorded, a field "prev" that contains the hash of the previous block and the field "hash" that corresponds to the encryption of the data using the selected algorithm.

<sup>8</sup> <https://andersbrownworth.com/blockchain/>

<sup>9</sup> [https://en.bitcoinwiki.org/wiki/Merkle\\_tree](https://en.bitcoinwiki.org/wiki/Merkle_tree)

<sup>10</sup> <https://github.com/tendermint/tendermint/wiki/Block-Structure>

*Figure 2 - Creation and validation of blocks*

The figure displays three sequential block creation forms, each with a green background. Each form contains the following fields: Block #, Nonce, Data, Prev (previous block hash), Hash, and a Mine button. Block 1 has a Nonce of 11316 and a Hash of 000015783b764259d382017d91a36d206d0600e2cbb3567748f. Block 2 has a Nonce of 35230 and a Hash of 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd844. Block 3 has a Nonce of 12937 and a Hash of 0000b9015ce2a08b61216ba5a0778545. The Prev field of each block contains the Hash of the previous block, demonstrating a valid chain.

Block #	Nonce	Prev Hash	Hash
1	11316	00	000015783b764259d382017d91a36d206d0600e2cbb3567748f
2	35230	000015783b764259d382017d91a36d206d0600e2cbb3567748f	000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd844
3	12937	000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd844	0000b9015ce2a08b61216ba5a0778545

As we can see from this figure, all blocks are valid since the hash of the previous block always corresponds to the hash in the field “prev” of the following block.

But, If for instance, data is changed within any of these blocks, like in the figure below, all the following blocks are invalidated, since the change in data changes the hash of the block, resulting in an incongruence with the hash in the field “prev” of the block following.

*Figure 3 - Immutability of data*

The figure displays three sequential block creation forms, each with a pink background. Block 1 is identical to the one in Figure 2. Block 2 has its Data field changed to 'change here', which results in a new Hash (3251f73cbdf725375b3319ab53ce835084f3fbd4af02881e2). Block 3's Prev field still contains the original Hash of Block 2, which no longer matches its own Hash, indicating an invalid chain.

Block #	Nonce	Data	Prev Hash	Hash
1	11316		00	000015783b764259d382017d91a36d206d0600e2cbb3567748f
2	35230	change here	000015783b764259d382017d91a36d206d0600e2cbb3567748f	3251f73cbdf725375b3319ab53ce835084f3fbd4af02881e2
3	12937		3251f73cbdf725375b3319ab53ce835084f3fbd4af02881e2	704d2a0b1ed22be3e53d9e22614f077d

### 1.3. Key system and digital signatures

Digital signatures, which encrypt transactions, are computational schemes divided into two parts: the algorithm for the creation of the signature, which utilizes the private key to sign the message, and the algorithm for verifying the signature, which uses the public key.

Three tasks must be completed by a digital signature:

- Show concrete evidence that the person owns the funds and has therefore the authority to spend them.
- Attest the validity of the authorization proof.

- The signature establishes that the transaction cannot be altered once it has been signed.

The verification algorithm examines: the message, the public key that agreed to sign it, and the signature, and returns true if the signature is legitimate for that specific message and public key.

The digital key, the Ethereum address, and the digital signature are used to prove possession of Eth (the native coin of Ethereum). The network does not keep digital keys; instead, users generate a file and save it locally or in their wallet. Each transaction must be authenticated by a digital signature issued by a private key whose possession allocates control and certifies the ownership of the Bitcoin included in the transaction in order to be inscribed in a blockchain.

The system is built on a sophisticated asymmetric key scheme that uses two kinds of keys, public and private, to perform encryption and decryption. They're linked to a cryptographic system based on a mathematical function (e.g., Elliptic Curve Multiplication<sup>18</sup>), which is a one-way (irreversible) function since it is easy to calculate in one direction but impossible in the other.

This is an example of a private key:

“a167b607bi8caf03ecf1f2c3t20098a3ceb12e1fdae7b4111e82c73cb3440055”

This is an example of a public key:

“0x7277Fc6ee8B4419fdC60346981cB6FC11F6b5913”

## 1.4. Wallet

Blockchain is associated with cryptocurrencies and wallets, and it is used as a payment protocol for sending and receiving payments<sup>11</sup>. Bitcoin is a digital currency that is used to store and transfer value among people involved in the Bitcoin network. It is used to buy and sell goods and services, transfer money to individuals or organizations, and extend credit, just like any other conventional currency. It can also be sold, purchased, and exchanged for other currencies, just like any other conventional currency. In contrast to traditional currency, Bitcoin is entirely digital, and users have their own private key, which allows them to prove their ownership of the Bitcoin stored in their wallets, thereby enabling transactions. This key is required to unlock the wallet and spend the cryptocurrencies in transactions. Keys are typically stored in a digital wallet<sup>12</sup>, which can be found on the owner's hardware devices.

---

<sup>11</sup> <https://consensys.net/blog/metamask/>

<sup>12</sup> <https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys>

The market currently provides several different types of wallets, each of which differs in terms of the platforms on which it is used and the difficulty with which it is used. They can be divided into the following categories:

- **Desktop wallets:** the very first category of wallet ever created; they can be used on both Windows and MacOS operating systems simultaneously. They must have been chosen because of their greater autonomy and control, even if lacking in terms of security and configurations.
- **Mobile wallets:** the most commonly used type of wallet; they can be accessed through smartphones running the iOS or Android operating systems and are distinguished by their straightforward design and fluid user experience.
- **Web wallets:** they are wallets that are kept on a server that is controlled by a third party and are available through a web browser. Most of them are based on systems which work by executing portions of the code on the user's terminal, allowing them to control the keys in their possession.
- **Hardware wallets:** they are contained inside of hardware devices that communicate with the ledger through NFC or USB technology. Considering their characteristics, these are praised for their security as well as their ability to hold large sums of money in their pockets.

Printing the digital keys (cold storage) on paper allows to securely keep digital keys for a long period of time.

## 1.5. Consensus mechanism

As previously stated, blockchain is essentially a network-work-distributed database in which nodes constantly capture information in "blocks," which are then assembled into one "chain". To accomplish decentralized consensus, one party no longer needs to depend on a central authority or rely on the other party in order to share information with the other (transfer of value is considered as information as it concretizes itself in a transaction)

During this time period, a large number of consensus mechanisms have been developed, recently the number of consensus mechanisms has spike. As a result, due to the non-technical disposition of this work, I will go through to the most popular and traditional, namely Proof of Work and Proof of Stake.

### 1.5.1. Proof of Work (PoW)

Bitcoin uses the most well-known mechanism for obtaining consensus on a blockchain<sup>13</sup>. Unlike others approaches, Proof of Work does not need all nodes on a network to give their respective judgments in order to reach a consensus. Instead, PoW employs a fixed-size hash function (which converts a string of characters

---

<sup>13</sup> Mastering Bitcoin 2nd Edition - Programming the Open Blockchain, 2018

into a shorter fixed-length value representing the original string which is used to find items in a database) to create conditions in which a single participant is allowed to unveil their conclusions about the submitted data, and those conclusions can then be checked by all the network participants. The irreversibility of the hash function is a major factor for its use. A hash function cannot be reverse-engineered. Indeed, the hash function's parameters prevent misleading conclusions from being reached, ensuring that fraudulent data cannot be computed in an appropriate manner. As a result, creating a proof of work becomes a random process with a low chance of succeeding, requiring an average of significantly numerous trial and error before a legitimate proof of work is formed. This means that each user knows and can independently verify that a particular amount of labor is deployed to create a new block; for a malevolent actor to alter the ledger, it will need to have more computational power than the whole network has.

### **1.5.2. Proof of Stake (PoS)**

The fact that mining is done by all players in the ecosystem who have a vested interest in the ecosystem is a fundamental justification for choosing a proof of stake mechanism. Specifically, rather than any individual simply trying to calculate a value in order to be selected to “solve” a block - like in Proof of Work - the network makes the decision about which member announces the results, and system participants are automatically and exclusively entered into that lottery based on their total stake in the network<sup>14</sup>. This “lottery” makes decisions based upon the amount of value staked by the participant, the time the participant has spent in the network, the rate of the participant (based on previous validations) and combines all together with a factor of randomness. Polygon is an example of a blockchain that use this consensus process, but recently, also due to the high energy required by PoW blockchains, many new protocols are adopting the PoS or its many variants (e.g Pure PoS). Indeed, with its new upgrade "ETH 2.0," Ethereum intends to move from PoW to PoS changing completely the Blockchain ecosystem as Ethereum is the second cryptocurrency by market cap and is losing dominance to other new protocols due to the fact that the latter, using proof of stake, can provide speedier transactions and almost insignificant fees. With Ethereum moving to proof of stake, and all the value locked in the ecosystem many new applications can flourish benefiting from lower transaction costs and more practicality.

---

<sup>14</sup> "Da Zero alla Luna. Quando, come, perché la blockchain sta cambiando il mondo", Gianluca Comandini, 2020.



## 1.6. Blockchain enablers

We have now established some of the core concepts underlying Blockchain technology and cryptography, therefore in the following sub-chapters are outlined the enablers of the technology, or, the main possibilities that Blockchain allows, namely: notarization, tokenization and use of smart contracts.

### 1.6.1. Notarization

To begin, it is necessary to clarify that the term "notarization" (or "legalization") of a document refers to the process by which the authenticity (or originality) of the document in question is attested, as well as the document's existence based on a specific date and time ("timestamp"), in such a way that it results trusted.

Essentially, the activity is composed of three phases: control, certification, and record preservation. The significance of this function is inextricably linked to the requirement for security and dependability in internal relationships with social organizations. Throughout history, these individuals have entrusted intermediaries with the responsibility of carrying out these processes, particularly in light of the trustworthiness that their role has acquired over time.

Most of these services (offered exclusively by notaries, banks, and government agencies that manage public records) are also predicated on the existence of records attesting to the existence of transactions between two or more counterparties at a specific point in time. However, over time, more attention has been paid to instances in which the intermediary has been implicated in record-keeping violations, particularly since his incentives to operate in an ethical manner are aligned more with his personal interests than with those of the system. As a direct result of these behaviours, over time, there has been a progressive erosion of trust throughout the system and an increase in the complexity of managing these operations, so making the social ecosystem intrinsically less secure. The value of notarial services is based on the fact that their result is legally valid. Due to the fundamental characteristics of the blockchain, it enables the "globalization" of trust between diverse parties by disseminating a perception of the registrant's trustworthiness while also ensuring the security of personal information. The blockchain may be able to eliminate inefficient commissions associated with notarial services.

As we have seen before, every time that information is added to a block a hash is generated, when information inside the block is altered or cancelled, even if by a minimal change, the hash changes completely, invalidating all the blocks that follow. Notarization on blockchain builds on this feature of immutability, once an asset is "notarized", information related the asset is added into a block contributing to the creation of the related hash. Therefore, the hash guarantees the existence and the data of the asset (Proof of Existence). Then, once an asset

is transferred from one owner to another, this transaction's related information are inserted into another block, contributing to the creation of its related hash which basically guarantees the transfer of the ownership.

To attest the existence and the ownership of a given asset are the two main benefit that come from the notarization, which, seen from an higher level perspective can be seen as the elimination of the need for an attestation from trusted party.

### 1.6.2. Tokenization

To understand the concept of a "blockchain token" it is necessary to understand what we are talking about when we refer to the word Token. In general, tokens in the context of blockchain can represent an asset, a right or anything else related to the real world. The value of a blockchain token may depend on a specific link to the "fixed assets" it represents. They can be anti-inflationary, i.e. have a nominal value that expresses the link between the value of the underlying asset and the native blockchain asset.

Secondly, we can differentiate tokens on the basis of their purpose, We can thus distinguish between: "usage tokens", which give their owner access to a digital service (without any centralized control); "work tokens", which allow the holder to contribute to the operation of a network; "funding tokens" that have the objective of raising funds; "staking tokens," which refer to the potential use of tokens to gain the right to participate in a network decision making process (as seen in more detail in the paragraph "Proof of Stake").

In general, to provide greater clarity, we can identify three macrocategories: fiat Pegged Token, Utility Token and Asset Backed Token.

- Fiat Pegged Token, also referred to as stablecoins, are a digital representation of fiat currencies, examples of stablecoins are DAI, USDC, USDT. Their price is pegged to fiat currencies' price.
- Utility Tokens provide digital access to an application or service.
- Asset Backed Tokens (whose issuance is called STO, Security Token Offering) are essentially the digital representation of assets, or rather they are equivalent to a right to be transformed into the underlying asset to which greater liquidity and transferability has been conferred via the blockchain

In general, the Ethereum platform enables the management of tokens that adhere to a common standard (ERC20) and are capable of performing a broad range of functions and representing a diverse range of digital assets; by adhering to the same standard, the tokens can be easily identified within the Ethereum ecosystem.

The digitization of an asset enables the creation of a consolidated view of the asset at multiple levels of detail; for example, this can occur at the departmental or enterprise level within an organization, at the industry level

for regulators, or at a much higher economic level for various types of assets. However, since the assets are quite distinct from one another their tokenization will require consideration of a variety of factors.

We begin by considering a high-value asset, such as real estate, for which a securitization operation is sought in order to sell property quotes to small investors. In these instances, the asset will be placed in a fund, the quotes of which will be used to denote the asset's ownership; however, through tokenization, each token could be associated with a quota associated with the asset's respective ownership right. The advantage in this case is that it is linked to an increase in liquidity via the expansion of the pool of investors. The tokens used in this procedure are fungible, which means that each of them confers the same rights as the others, has the same value, and is interchangeable.

In a second context, it is possible to tokenize non-fungible assets such as nominative documents; in these instances, each asset is associated with the possession of a single token with characteristics that render it unique and non-transferable, thereby constituting the asset to which the reference is made.

Finally, it is possible to tokenize unique assets that have a commercial value and are frequently held for the purpose of being resold; in this case, the so-called "digital goods" can be acquired and managed entirely online via specialized platforms. This latter type of tokenization may be particularly appealing in certain corporate contexts where falsification is a problem and therefore it is necessary to ensure the "unicity" or, more precisely, "non-reproducibility" of the underlying assets. Thus, we can assert, in general, that the issuance of a blockchain-based token follows a methodology that is quite similar, in many ways, to the traditional process of securitization. The latter is the process referring to the creation of the so called No-Fungible Tokens, which have recently saw great adoption and created a whole new market with monthly volumes of sales going beyond \$3b<sup>15</sup>.

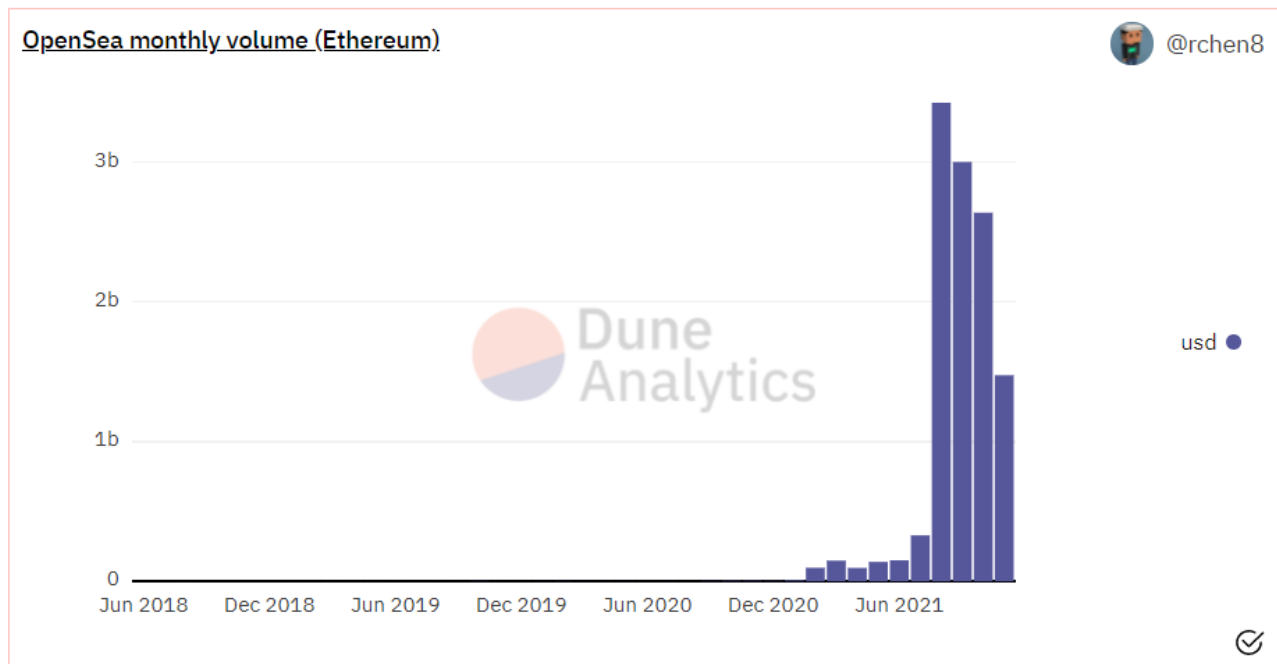
In the graph below we can see the monthly volumes of Opensea<sup>16</sup>, the biggest marketplace for NFTs.

---

<sup>15</sup> <https://www.fintechna.com/articles/nfts-and-the-cryptoverse/>

<sup>16</sup> <https://opensea.io/>

*Figure 4 - Monthly NFT volumes in USD on OpenSea*



*Source: Dune Analytics (2021)<sup>17</sup>*

From what just explained we can infer that it is possible to create a "Token Economy" capable of providing the opportunity to create a more efficient and fairer financial ecosystem through a significant reduction in the presence of traditional financial frictions. Indeed, one may identify four primary benefits of tokenization: increased liquidity, faster and less expensive transactions, increased transparency, and a higher level of accessibility. Following the operation of tokenizing an asset, particularly one that is private or typically illiquid (such as fine arts), the corresponding tokens may be traded on a secondary market selected by the issuer of the asset, granting access to a broader range of individuals. This may increase liquidity, benefiting both the investors, who will have increased freedom, and the vendors, as the token benefits from a liquidity premium, thereby capturing a higher value than the underlying asset.

The exchange of a token is completed via the use of a smart contract, which automates some of the transaction's steps; this automation is capable of reducing the amount of administrative overhead required, while also requiring fewer intermediaries, resulting in not only a more rapid execution of the operation, but also lower transaction costs. Additionally, the tokens may be capable of incorporating not only a specific legal right for the detainee, but also the associated legal responsibilities, in conjunction with an immutable proof of ownership.

These characteristics have the potential to increase the transparency of transactions by enabling each party to understand who the exact counterparty is, what their own rights are, as well as to obtain information about who

<sup>17</sup> <https://dune.xyz/rchen8/opensea>

previously detained the token. The final and most significant feature is represented by the tokenization's capacity to expand investment opportunities in underlying assets by lowering the required minimum investment amount and duration.

Due to the divisibility, investors can acquire a token that represents an absurdly small percentage of the underlying asset, hence lowering the cost of the investment and increasing liquidity, due to the facilitation of trading on more global secondary markets. All of this defines a new ecosystem characterized by a high degree of personalization and customization of investments.

### **1.6.3. Smart Contracts**

The introduction of smart contracts was a significant breakthrough to boost the adoption of blockchain.

Smart contracts are pieces of code that are recorded on a blockchain and execute actions based on predefined conditions. They allow counterparties to automate operations that were previously handled manually through a third-party mediator. Smart-contract technology has the potential to accelerate corporate operations, minimize operational errors, and increase cost efficiency.

For example, two parties might use a smart contract to join into a shared derivative contract to hedge the price of gold at a given time.

Once the contract conditions are agreed upon, it is added to the blockchain, and the staked amounts are locked and recorded on a blockchain. At the given time, the smart contract would read the price of gold from a trustworthy source specified in the smart contract (this source is called "oracle"), compute the agreed amount, and send cash to the right party on the blockchain. Ethereum, the 2nd biggest blockchain network behind Bitcoin in terms of market capitalization at the time of publishing, was the first platform to deploy a smart contract that could be installed and operated on a decentralised network. Ethereum is a public blockchain that allows anybody with access to it to read the details of each transaction. This might be a concern for contracts that have confidential data (e.g., a hedge fund using smart contracts to follow a proprietary investment strategy or to privately set a position in a specific market). Developers, therefore, are actively exploring methods to maintain secrecy while utilizing public blockchains. Even with these apparent limits, smart contract applications have substantial market potential across sectors since they are able to improve efficiency of the processing and settlement of a broad variety of contracts, from traditional financial operations to automatic leases, cryptocurrencies exchanges and insurance. Smart contracts are a way of automating the contracting process and permit minimum human participation in oversight of contractual commitment. Automation can increase efficiencies, reduce working hours and operational failures. Because smart contract

technologies require all contractual provisions to be translated into logic, contractual fulfilment can also be improved in certain instances by eliminating ambiguity.

Innovative hazards that need to be managed might arise as smart contracts adoption and development continue to grow. For example, the counterparties may opt to exclude all conceivable outcomes while putting up a smart contract or they might include a certain amount of flexibility, so that they are not limited. This might result in smart contracts with weaknesses or mistakes leading to unforeseen business results. Because of an unavoidable mistake, parties may have difficulty renegotiating the terms of an agreement or amending terms. Incomplete or excessive contracts may also lead to issues and conflicts of settlement. Most significantly though, smart contracts were not fully tested in the legal systems. Smart contracts, nonetheless, provide an overwhelming argument for blockchain use.

Since all companies collect information and confront the issue of reconciling data with peers, blockchain technology can be useful to all. Yet, the first significant adoptions can alter outdated and lengthy corporate processes and legacy systems.

The main enablers of Blockchain technology have been presented, and they are: Tokenization, Notarization and Smart Contracts. Nowadays, everyone appears to be fascinated by the prospect of incorporating blockchain technology into their current business model or utilizing blockchain technology to solve existing problems. Blockchain, on the other hand, cannot be used in every situation. Businesses must conduct a thorough analysis of their current business problems before implementing this new and promising technology.

Below is illustrated a high-level framework, made up by three main steps, that can help companies analyse whether they could benefit from the adoption of Blockchain technology.

**Step 1:** Identify the ecosystem the company is in. This means have a clear idea of all the stakeholders involved in the core business processes.

**Step 2:** Analyse whether there's the need for a trusted framework to be adopted. If there is no need for trust between parties, or parties already trust each other completely, then Blockchain would lose its added value; therefore, more traditional automation systems would suit better.

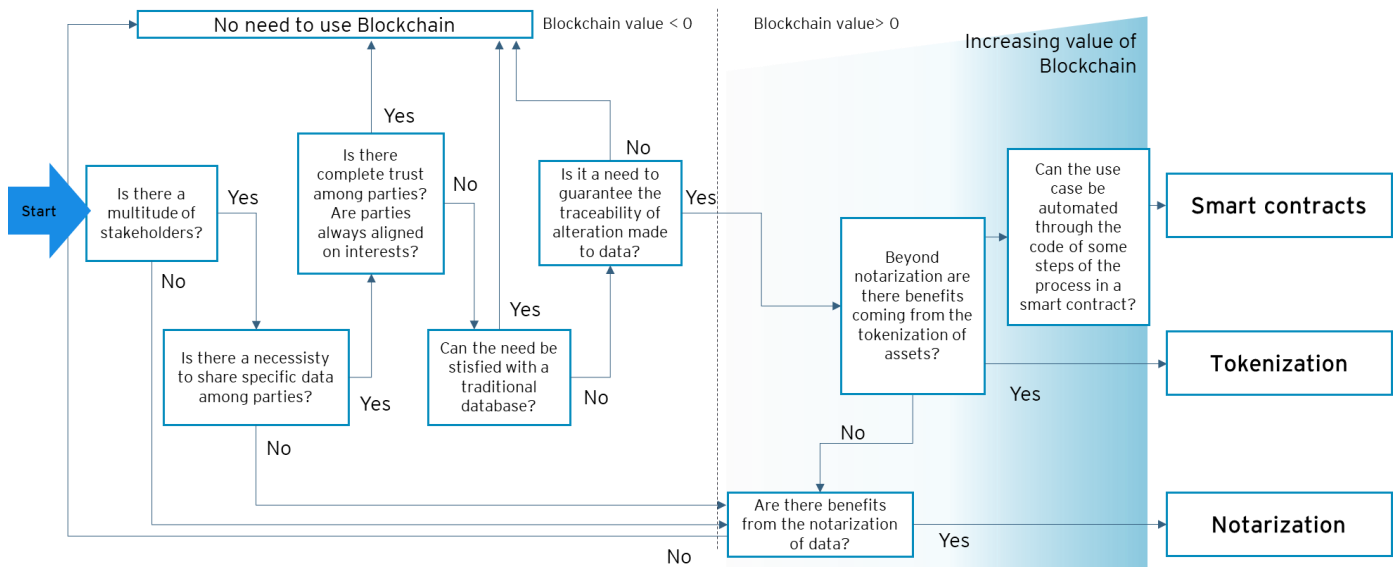
**Step 3:** Once it has been understood that the company would benefit from the use of blockchain, it is time to understand which are the benefits that the company is actually looking for.

- Smart contract, as stated before, can help companies automate their processes by adopting a “if/then” approach tailored to the specific use case by implementing specific rules into them.
- Tokenization: tokenized assets can be exchanged throughout the value chain and carry information that can be updated in each step of it. The tokenization of assets is used in traceability solutions, where, through

the use of Non-Fungible Tokens (NFT) products can be tokenized and carry with them the whole production processes related information.

- Notarization, among the three, is the one that affects the least existing processes, yet bringing an incredible value to ecosystems composed of different stakeholders that need their interactions to be trusted.

*Figure 5 - Decision making process to adopt Blockchain*



## 1.7 Blockchain typologies

The hardware that supports blockchains can be owned by two sorts of entities: public and private. The distinction between public and private blockchains is analogous to the distinction between the Internet and intranets. The Internet is a freely accessible resource. There is no barrier to accessing it; there is no gatekeeper. Intranets, from the other side, are private information transmission networks used by corporations. Private blockchains are comparable to intranets, whilst public blockchains are similar to the Internet. Yet both are valuable in today's world, there's no denying that the Internet has way more impact in the world than the Intranet.

The crucial distinction is just how the parties get access to the network. Consider the fact that a blockchain is generated by a decentralized system of computers that employs encryption and a consensus mechanism to maintain the community members in synchronization. If isolated, a blockchain is worthless; a data warehouse would suffice. A blockchain's community of computers can be either public or private, also known as respectively permissionless or permissioned.

### 1.7.1. Public blockchain

Bitcoin is an example of a public system, in which anybody with the appropriate hardware and software may join the network and access the data stored there.

To access it, there is no gatekeeper verifying IDs. Furthermore, network involvement creates an economic equilibrium in which entities would acquire additional hardware to participate in the construction of Bitcoin's blockchain if they believe they can profit from it. Ethereum, for instance, is another example of a public blockchain, together with Cardano and many others.

There are a lot of public blockchains out there, and they're all distinct. Some members of the early Bitcoin network believe that the defi

nition of a blockchain should be quite strict, and that any blockchain must utilize proof-of-work as a consensus mechanism. I personally disagree with such limited viewpoint since many alternative intriguing consensus mechanisms, such as proof-of-stake give opportunities for the further adoption of this technology, such as scalability, less energy consumption and improved transaction speed. To strengthen my opinion, Ethereum, the second cryptocurrency by market cap<sup>18</sup> at the time of writing, is now working to shift its whole network toward the use of PoS (proof of stake), due to rising concerns about the sustainability of the usage of the Blockchain technology and its scalability issues<sup>19</sup>.

### **1.7.2. Private blockchain**

On the other hand, private networks need permissions to be accessed. Only entities with the appropriate permissions are allowed to join the network. These private systems arose after Bitcoin, when corporations and enterprises recognized that while they enjoyed the usefulness of Bitcoin's blockchain, they found many issues, business and legal related, to be as open with the information shared with public institutions.

In the financial services industry, private blockchains are primarily solutions devised by incumbents in a bid to maintain their position. While several of these ideas have validity, others argue that the biggest revolution has been bringing huge and secretive companies together to share knowledge and best practices, lowering the cost of services to the end customer. Because of the trend to open networks, I personally believe that the adoption of private blockchains will weaken the dominance of centralized big players over time. To put it another way, it's a step toward more decentralization and the usage of public blockchains.

---

<sup>18</sup> <https://coinmarketcap.com/exchanges/blockchain-com-exchange/>

<sup>19</sup> <https://bit-news.ch/2021/07/ethereum-heads-to-100k-tps-buterin-talks-about-post-merger-future/>



Private blockchains have a wide range of potential uses outside of the financial services industry. Given that the use cases for a solution that specializes in protecting transactions are naturally clearer, banks and other monetary intermediaries have been the fastest to implement the technology. Aside from the financial services sector, the food industry, insurance, healthcare, digital identification, and a variety of other industries are experimenting with blockchain technology; those will be further analysed in the following chapter.

### **1.7.3. Hybrid blockchain**

Finally, hybrids are a form of private blockchain run by a group rather than a single business and in which all participants are identifiable. They essentially function as a somewhat decentralized platform. Some of the nodes are "predetermined," rather than having anybody with an internet connection participate in the transaction verification process, or giving a single company full power. These nodes are in charge of the consensus process, therefore they may read and/or write data and decide who has access to the blockchain ledger. The right to read might be open to the public or just available to participants. For example, in a consortium of a few firms, if one of them trades and wishes to share information solely with some of the other companies in the network, the right to read might be limited to the participants. If there is a group of a few firms, and one of them trades and wants to share information with only a few of the other companies in the network, they can be expected to be the only ones who can view the shared data. The aim to magnify the qualities of the technology associated to its nature as a distributed ledger, in order to boost collaboration and improve procedures across diverse organizations, such as banks, enterprises, and government agencies, has led to the usage of this sort of blockchain. Hybrids, like private blockchains, are platforms with an authorization system that permits access only to those with permission, allowing participating institutions to keep a certain amount of control and privacy. Many organizations are hesitant to put confidential information about their business on a platform that is public, unlicensed, and thus available to anybody. Hybrid blockchains are common in the international commerce industry.

### **1.7.1. Bitcoin Blockchain**

The Bitcoin protocol is based on the blockchain technology. Bitcoin's pseudonymous developer, Satoshi Nakamoto, described the digital currency in a research paper presenting it as "a new electronic cash system that is completely peer-to-peer, with no trusted third party."

The critical point to remember is that although Bitcoin utilizes blockchain to create a transparent ledger of payments, blockchain may theoretically be used to immutably record any amount of data items. As said before, this might take the shape of transactions, goods inventories, digital identity and verifiable credentials.

Currently, tens of thousands of projects are exploring methods to use blockchains in ways other than transaction recording, several of which will be discussed in the next chapter.

As clarified above blockchain is the enabling technology that allows the Bitcoin network to work. Bitcoin is both the name of the network and the name of the cryptocurrency used within the very network, this is the reason why many people tend to not spot the difference between the cryptocurrency and the technology used to enable the exchange of the cryptocurrency.

Cryptographers and innovators have attempted to build an actual currency for online transactions since the internet's inception. After the financial crisis of 2008, the bitcoin whitepaper was released. It was a unique approach that integrated cryptography and distributed systems advancements.

The bitcoin network is an electronic payment system that uses cryptographic evidence rather than trust to allow any two willing parties to interact directly with each other without the use of a trusted third party. Bitcoin is the internet of money, to put it simply.

### **1.7.2. Ethereum Blockchain**

The term "global computer" is frequently used to describe Ethereum. But what exactly does that imply? Let's start with a computer science-focused explanation, and then compare Ethereum to Bitcoin and other Blockchains.<sup>20</sup>

Ethereum is a deterministic but virtually unlimited state machine, comprised of a globally accessible singleton state and a virtual machine that implements modifications to it.

In a more practical sense, Ethereum is an open source, worldwide decentralized computer platform that runs smart contracts. It makes use of a blockchain to synchronize and record state changes that occur in the system, as well as a cryptocurrency called ether to track and limit execution resource costs.

Ethereum has several aspects in common with the rest of open blockchains, including a peer-to-peer network, a PoW blockchain, the usage of cryptographic features like digital signatures and hashes, and a cryptocurrency (ether).

Yet, in many respects, Ethereum's aim and design diverge markedly from those of the open blockchains that came before it, including Bitcoin.

---

<sup>20</sup> <https://ethereum.org/en/>

Ethereum's primary goal is not to create a crypto exchange network. Although the digital currency ether is crucial to the effectiveness of Ethereum, it is designed as a utility currency to pay for the usage of the Ethereum platform as the global computer.

In contrast to Bitcoin, which has a relatively restricted scripting language, Ethereum is intended to be a general-purpose programmable blockchain with a virtual machine capable of running code of unlimited and limitless complexity. Whereas Bitcoin's coding language is purposefully limited to basic true/false assessment of payment conditions, Ethereum's language is "Turing complete", which means that Ethereum potentially acts as a general-purpose computer.

The Ethereum platform alone lacks capabilities and is value-agnostic. It's indeed up to companies and programmers to decide what it should be used for, much like computer languages. Yet, it is evident that some application categories benefit from Ethereum's features more than some other. Specifically, Ethereum is well-suited for use cases that automate peer-to-peer contact or allow synchronized group activity across a network. Applications for managing peer-to-peer markets, for example, or the automation of complicated financial transactions.

Bitcoin enables individuals to trade money without the involvement of any intermediaries such as financial organizations, banks, or governments. Ethereum's influence might be further-reaching. Conceptually, financial transactions or trades of any complexity might be performed automatically and safely using Ethereum programming. Beyond financial applications, the Ethereum platform may have a significant influence on any environment where trust, safety, and permanency are crucial — for example, asset-registries, voting, governance, and the IoT.

Ethereum integrates many tools that Bitcoin users will be already acquainted with, while it also brings numerous changes and innovations of its own. Whilst the Bitcoin blockchain is simply a record of transactions, the account is Ethereum's fundamental unit<sup>21</sup>. Every account's state is tracked by the Ethereum blockchain, and all state changes on the Ethereum blockchain involve transfers of value and/or information across accounts. The latter are classified into two types:

- Externally Owned Accounts (EOAs): accounts that are managed via private keys.
- Contract Accounts: governed by their contract code (smart contract) which must be somehow activated by an EOA.

Transactions, like in Bitcoin blockchain, need the payment of a fee to incentivize the network (in addition to the incentive for mining a new block) and maintain the security of the network. Those are paid at each stage by the individual who executes the transaction in ether (ETH). The nodes that approve the transactions receive

---

<sup>21</sup> <http://ethdocs.org/en/latest/introduction/what-is-ethereum.html>

fees. Miners are the entities that accept, disseminate, validate, and execute transactions in the Ethereum and Bitcoin models, respectively.

### 1.8.3. Ripple Blockchain

Ripple is a fintech company located in San Francisco that is responsible for the RippleNet global payments network, as well as the XRP Ledger blockchain and its native digital asset, XRP<sup>22</sup>. In 2004, a computer programmer named Ryan Fugger came up with the concept for Ripple. Ryan imagined a decentralized monetary system in which groups might create their own currency. RipplePay was created out of his idea of establishing an Internet of Value. Early on, RipplePay had considerable success, but the network was small and the software was centralized. As a result, RipplePay partnered with Open Coin, a project launched by Jed McCaleb, who is now with Stellar, and Chris Larson, in 2012.

Ripple came into being when Open Coin and RipplePay merged to become what is today known as Ripple. RippleNet is a fintech enterprise solution for financial institutions that enables users to send, receive, retain, and move currencies across borders faster and more reliably. RippleNet<sup>23</sup> solves the problem of old financial systems and networks being fragmented and slow. Many of these networks are not integrated among banks, and no significant breakthroughs in any system have happened in decades. This is where RippleNet comes into play. Ripple is a fast, secure network that can settle transactions in 3 to 5 seconds from anywhere on the planet, far faster than Bitcoin or Ethereum<sup>24</sup>. It can process 1,500 transactions per second and scale to the same rates as the Visa payment system. RippleNet does this in a variety of ways<sup>25</sup>. Ripple employs the open-source XRP Ledger blockchain to track, process, and cryptographically guarantee all transactions. However, unlike Bitcoin, XRP does not use Proof of Work or have a mining concept. This means that the blockchain consumes relatively little energy and, as a result, transaction costs are likely to remain cheap.

XRP transactions are managed by an independent community of validating nodes, who maintain the network and transaction protocol up to date.

To maintain the network's integrity, users can select trustworthy validators from a Unique Node List, or UNL, which is a publicly recognized and recognizable list of trusted nodes such as Microsoft and MIT. The UNL ensures that no single organization has the ability to control the network, and it forbids members from attacking it jointly. Moreover, half of the validators on Ripple's recommended UNL are run by nodes outside the company, and the list is updated on a regular basis with new independent validators.

---

<sup>22</sup> "The Ripple Protocol Consensus Algorithm", Ripple Labs Inc., 2014.

<sup>23</sup> <https://ripple.com/rippletnet/>

<sup>24</sup> <https://ripple.com/xrp/>

<sup>25</sup> <https://www.fool.com/investing/2018/02/01/3-cryptocurrencies-processing-1500-or-more-transac.aspx>

Ripple is also anti-money laundering compliance, with fraud detection, sanction screening, and regulatory reporting capabilities, which is exactly what banks want. As a consequence, RippleNet has shown to be a secure, robust, and stable network with long-term stability and governance.

Within the Ripple network, XRP — the digital currency on the XRP Ledger<sup>26</sup> — provides financial service providers with On-Demand Liquidity. XRP serves as a bridge currency for cross-border payments, replacing Nostro and Vostro accounts and eliminating the need for pre-funding.

For example, Bank A will convert its fiat currency to XRP and use XRP as a bridge currency to exchange with Bank B's fiat currency. In this case, XRP takes the role of the US Dollar as the base currency, but at a far cheaper cost and with no foreign exchange fees.

At today's prices, the transaction cost for XRP is 0.00001 XRP, which is less than \$0.01 per transaction. Payment firms might utilize XRP to grow into new markets, gain speedier payment settlements, and reduce their overall foreign currency costs.

Ripple is a contributor to the XRP Ledger, which is open-sourced and maintained by a global community of volunteers.

XRP is the On-Demand Liquidity option available to RippleNet customers, and it is one that Ripple, the firm, is promoting vigorously.

---

<sup>26</sup> <https://xrpl.org/>

## CHAPTER II – BLOCKCHAIN APPLICATIONS

Even though Blockchain is usually associated with cryptocurrencies, specifically Bitcoin, thus associating it with the only use case of peer to peer payments, it has a huge number of other use cases, some of them related to finance some others in completely different sectors. Blockchain has an enormous potential for building trust within ecosystems, no matter the sector in which they are, as well as bringing added value for end users/consumers of a given product. The use cases that are outlined in this chapter are very different one from the other, and this was purposely done in order to showcase the potential of the technology and to give the reader the idea of how it can be applied to any sector regardless the need for the use of cryptocurrencies. Naturally, the sectors targeted in this work which are: Decentralized Finance, Traceability, Digital Identity and Accounting, are not exhaustive, Blockchain can and is already applied to a vast number of other areas, but it would not be possible to analyse all of them in depth in one single research.

At the end of this chapter are outlined the results of a survey done by EY on 100+ C-Levels of both the public and private sector on Blockchain adoption in general and on these specific sectors of application: Decentralised Finance, Traceability and Digital Identity.

### 2.1 Decentralized Finance (DeFi)

DeFi, or decentralized finance, is a movement aimed at creating a new financial system that is accessible to everybody and does not rely on trusted middlemen such as banks. To do this, defi largely depends on encryption, blockchain technology, and smart contracts. Smart contracts are the fundamental tenets of defi.

It's important to note that the majority, if not all, defi projects are now based on Ethereum. The primary reason for this is Ethereum's reasonably strong coding language, Solidity<sup>27</sup>, which enables the creation of advanced smart contracts capable of containing all of the logic required for defi. Additionally, Ethereum has the most evolved environment of all smart contract platforms, with independent developers creating innovative solutions daily and the highest value locked in its protocols, which creates strong network effects.

To have an idea of the size of DeFi Total Value Locked or TVL<sup>28</sup>, is used to measure the adoption of a given protocol and measures the funds locked into that protocol. At the time of writing the TVL among all DeFi protocols is at \$239bn<sup>29</sup> according to DeFi Llama, one of the main data providers for this ecosystem, with the dominance of Curve equal to 8.8% (\$21.14bn). The TVL as of the 1<sup>st</sup> January 2021 was \$25.96bn, resulting in a growth of 856%, or approximately \$214bn in just one year<sup>30</sup>.

---

<sup>27</sup> <https://soliditylang.org/>

<sup>28</sup> <https://coinmarketcap.com/alexandria/glossary/total-value-locked-tvl>

<sup>29</sup> <https://defillama.com/>

<sup>30</sup> <https://defillama.com/chains>

MakerDAO<sup>31</sup> was one of the first initiatives to kickstart the decentralized financial movement. Launched in 2015, MakerDAO enables users to store collateral such as ETH and produce DAI - a stable currency that, via the application of specific incentives, tracks the US Dollar's price. This reintroduces one of the financial system's cornerstones — lending and borrowing. Indeed, defi is attempting to develop an entirely new financial landscape in an accessible and permissionless manner. Lending and borrowing are just a small component of this ecosystem. Stable currencies, decentralised exchanges, liquidity pools and margin trading are among the other critical components<sup>32</sup>.

### 2.1.1 Lending and Borrowing

Lending and borrowing are critical components of every financial system. Most individuals experience the need for borrowing at some time in their lives, often when they take out a loan to purchase a home, a vehicle, or to pay for their higher education.

The principle is fairly straightforward. Lenders provide money to borrowers in exchange for an interest rate on their deposit. Borrowers pay interest on the amount they need in return for rapid access to funds. Historically, lending and borrowing have been facilitated by the efforts of a financial institution.

Lending and borrowing are possible in the cryptocurrency world using DeFi protocols such as Aave or Compound or via CeFi firms, or centralized finance, and it functions in a manner remarkably similar to that of banks. For example, BlockFi<sup>33</sup> takes custody of deposited assets and loans them out to institutional investors like market makers or hedge funds, as well as to other platform users.

While the centralized financing model works, it is prone to the same issues as centralized cryptocurrency exchanges — namely, losing client funds due to hacking or other types of carelessness.

Additionally, one may argue that the Centralized Finance model directly contradicts one of cryptocurrencies' primary value propositions — self-custody of assets.

DeFi lending enables users to become lenders or borrowers in an entirely decentralized and permissionless manner while retaining total ownership of their currencies.

DeFi financing is built on smart contracts that execute on publicly accessible blockchains, namely Ethereum. Which is also the reason why, in contrast to the centralised and conventional models, Decentralised Finance

---

<sup>31</sup> <https://makerdao.com/en/>

<sup>32</sup> How to DeFi, Coigecko, 2020.

<sup>33</sup> <https://blockfi.com/>

lending is available to everyone with no need to provide personal information or trust other entities to keep cash.

Although Aave<sup>34</sup> and Compound<sup>35</sup> are the two primary loan protocols accessible in DeFi, the ecosystem is evolving, and those protocols are growing at a breakneck pace. Both of the aforementioned protocols operate by establishing money markets for certain tokens like as ETH, stable currencies such as DAI and USDC, and others. Users who want to become lenders deposit their tokens in a specific money market and immediately begin earning interest on their tokens at the current supply APY.

The given tokens are transferred to a smart contract and made accessible for borrowing by other users. The smart contract provides additional tokens in exchange for the provided tokens, which represent the supplied tokens plus interest. The underlying tokens may be redeemed for these tokens.

Additionally, it's worth noting that all loans in DeFi are overcollateralized, which means that users seeking to borrow cash must provide tokens as collateral that are worth more than the loan being sought.

It's natural to wonder why we're taking a loan if we're required to provide tokens worth more than the loan amount; this might all be resolved by just selling the amount we want to use as collateral and receiving 100% of the funds rather than just a portion of them.

There are a variety of motivations doing this, including avoiding or deferring capital gains taxes on their tokens or increasing leverage in a particular position via the use of borrowed money. Indeed, if you have x Bitcoin (BTC) in your wallet and anticipate that BTC will increase in value over the next time period, you may increase your exposure to BTC by taking a loan against your current BTC and obtaining a stable currency (e.g. DAI), and then buy more BTC using the borrowed DAI.

Naturally, there is a limit to the amount of money that may be borrowed, and this limit is determined by two primary factors:

The amount of money that is accessible for borrowing in a certain market. This is often not an issue in busy markets unless someone is attempting to borrow a large number of tokens.

What is the collateral value of the tokens supplied: The collateral factor establishes the maximum amount that may be borrowed depending on the collateral's quality. For example, DAI (a dollar-pegged stablecoin) and ETH have a collateral factor of 75% on Compound<sup>36</sup>. This implies that up to 75% of the value of the DAI or ETH delivered may be utilized to borrow more coins.

---

<sup>34</sup> <https://aave.com/>

<sup>35</sup> <https://compound.finance/>

<sup>36</sup> <https://medium.com/@gettyh/compound-finance-asset-risk-e4025487fcbb>



If a user borrows money, the borrowed amount must always be less than the value of their collateral multiplied by the collateral factor. If this criterion is met, there is no time restriction on the duration of a user's borrowing.

If the collateral value falls below the acceptable level of security, the user's collateral will be liquidated in order for the protocol (the smart contract) to refund the borrowed amount.

Interest earned by lenders and interest paid by borrowers are determined by the ratio of provided to borrowed tokens in a specific market.

Borrowers pay lenders interest, which means that the borrow APY (annual percentage yield) is more than the supply APY in a certain market.

This is also one of the primary distinctions between Compound and Aave. While both protocols provide variable supply and borrow interest rates, Aave additionally offers a constant borrow interest rate. While stable APY is set in the near term, it may alter over time to reflect changes in the supply/demand ratio of tokens.

To illustrate how the DeFi lending protocols function, the following is an example of how Compound handles this.

For instance, a user funds Compound with two ETH. Compound provides a specified token in return for two ETH, which reflects the deposit the user has made to the protocol; these tokens are called cTokens, and in the event of providing ETH, they are termed cETH.

How many cETH tokens will be distributed to the user? This is contingent upon the current exchange rate for the market in question, in this example, ETH. When a new market is launched, the rate of exchange between cTokens and the underlying tokens is set to 0.01. This is a hypothetical situation, but we may suppose that each market begins at 0.01. Additionally, we may predict that this exchange rate will continue to grow with each Ethereum block.

If the customer had provided two ETH at the market's inception, they would have gotten  $2/0.01=200$  cETH. Once the ETH market becomes operational, we may anticipate that the exchange rate will increase to, say, 0.011.

This equates to a user receiving  $2/0.011=181.81$  cETH. If the person redeems their ETH promptly, they should get around the same amount as they invested, which is approximately 2 ETH.

When a user has cETH, which is just another ERC20 token, he or she may transmit it anywhere. The primary distinction is that cETH is required to withdraw the underlying ETH from Compound. Additionally, cETH continues to accrue interest even after it is transferred from the wallet that began the deposit to another wallet.

The exchange rate would grow with each Ethereum block. The rate of rise is defined by the supply annual percentage yield, which is calculated as the ratio of provided to borrowed capital.

Assume that the exchange rate from cETH to ETH grows by 0.0000000001 with each block in our scenario. Assuming the growth rate remains constant for a month, we can readily determine the amount of interest that may be earned. Assuming we have an average of five blocks each minute, we get the following numbers:

We must add  $0.0000000001 * 5 * 60 * 24 * 30 = 0.0000216$  to the previous exchange rate.  $0.011 + 0.0000216 = 0.0110216$ .

The user would earn  $181.81 * 0.0110216 = 2.0038371$  ETH if they choose to redeem their ETH. Thus, the customer earned 0.0038371 ETH in a month, or around 0.19 percent on their ETH. It is critical to note that the quantity of cETH received by the user has remained constant, and only the exchange rate has permitted the user to redeem more ETH than was originally deposited.

When users borrow other tokens, they use their cTokens (or whatever other token name the protocol specifies) as collateral. While collateral collects interest, it cannot be redeemed or transferred while it is being used as collateral.

As previously stated, the loan amount is decided by the collateral element of the given assets. Additionally, there is a smart contract that analyses all collateral throughout the user's account and determines how much may be borrowed securely without being quickly liquidated. To ascertain the collateral's value Compound generates its own pricing feed from a number of very liquid exchanges.

If a user chooses to refund the borrowed amount and reclaim their collateral, they must also repay the interest that has accumulated on their borrowed assets. Interest accrued is defined by the borrow APY and is also automatically raised with each Ethereum block.

Liquidation happens when the value of the collateral offered falls below the allowed percentage; the following example may assist illustrate this:

If BTC is priced at \$50k and the admitted borrow percentage is 75%, users will be allowed to borrow up to  $\$50,000 * 0.75 = \$37,500$ . If the price of BTC goes below a certain level, which is fully disclosed to the borrower at the time of borrowing and is also adjustable by the borrower, resulting in higher/lower borrowing costs, the collateral is liquidated, which means the protocol sells the collateral to repay lenders.

While decentralized finance mitigates many of the dangers associated with centralized finance, it introduces new hazards, most notably smart contract risks (the risk that the code upon which the smart contract is based fails), but also rapidly fluctuating APYs. This might result in uninformed users who were not watching

compound interest rates on a daily basis being liquidated by being required to repay more than planned in the same time period.

### **2.1.2 Liquidity Pools**

Essentially, liquidity pools are aggregates of tokens secured in a smart contract. They promote trade by providing liquidity and are heavily used by many decentralized exchanges (DEXs). Bancor protocol is one of the earliest efforts to use liquidity pools, although they were extensively established by Uniswap.

Before going into detail about how liquidity pools function and what is an automated market maker (AMM), it is important to understand why these are needed. In the major cryptocurrency exchanges, such as KuCoin or FTX, trading is based on an order book concept. This is also how conventional stock exchanges such as the NYSE operate. Buyers and sellers place orders in an order book concept, buyers want to acquire a particular item at the lowest feasible price, while sellers seek to sell the same asset for the highest possible price.

To facilitate deals, both buyers and sellers must agree on a price. This might occur as a result of either a buyer increasing their bid or a seller dropping their price. However, if no one is willing to place orders at a mutually agreed pricing level or if there are insufficient funds/stocks/coins available for purchase market makers are required. Market makers are essentially businesses that support trade by constantly being available to purchase or sell a certain item. By doing so, they offer liquidity, ensuring that customers may always trade without waiting for another counterparty to appear.

The same model could also be applied to Decentralized Finance, but, with Ethereum gas fees prices and slow transaction process it would be prohibitively slow, costly, and almost invariably result in a negative user experience.

The primary reason for this is that the order book approach is strongly reliant on a market maker or many of them who are constantly prepared to "create the market" in a particular asset. Lacking market makers, an exchange quickly becomes illiquid and virtually useless by average customers. Additionally, market makers often watch an asset's current price by continually altering their pricing, resulting in a massive volume of orders and order cancellations being submitted to an exchange.

Having a throughput of about 13-16 transactions per second and a block time of between 11-20 seconds, Ethereum is not a feasible choice for an order book model. Additionally, each contact with a smart contract incurs a gas tax, which means that market makers would pay exorbitant amounts of money just by altering orders. This is the reason why something new was needed to be invented that would perform effectively in a decentralized environment with transactions costs, which is where liquidity pools solve these potential issues.

In its simplest form, a given liquidity pool contains two tokens, and each pool establishes a market for the pair of tokens. USDC/ETH is an example of a widespread Uniswap (one of the main decentralized exchangers) liquidity pool.

Once a new pool is formed, the first liquidity provider sets the pool's starting price. The liquidity provider is rewarded for supplying the pool with an equal number of both tokens. If the pool's starting price is different from the current market price, this presents an immediate arbitrage opportunity, which might result in financial loss for the liquidity provider. This principle of delivering tokens in an appropriate ratio applies to any other liquidity providers (LP) ready to contribute further to the pool at any given time.

When liquidity is provided to a pool, LPs are compensated with tokens known as LP tokens in proportion to the amount of liquidity provided to the pool. When the pool facilitates a deal, a 0.3 percent fee is given proportionately among all LP token holders to reclaim their locked funds, plus any accumulated fees, the liquidity provider must exchange with the protocol her LP tokens.

Each token exchange facilitated by a liquidity pool results in a price adjustment determined by a deterministic pricing algorithm. This method is sometimes referred to as an automated market maker (AMM), and various liquidity pools may utilize somewhat different algorithms.

The majority of liquidity pools, like as those utilized by Uniswap, use a constant product market maker algorithm that ensures that the product of the two provided tokens is always the same. Additionally, due to the algorithm, a pool may always offer liquidity, regardless of the size of the deal. The primary reason for this is because as the required quantity rises, the algorithm arithmetically raises the price of the token. The mathematics behind the constant product market maker determines the price; for example, if someone purchases BTC from a USDC/BTC pool, they lower the supply of BTC and increase the supply of DAI, resulting in a rise in the price of BTC and a reduction in the price of DAI. The amount by which the price changes is proportional to the size of the transaction in relation to the size of the pool. The larger the pool in contrast to a given transaction, the less the price effect (commonly referred to as "slippage"), which means that huge pools can absorb larger deals without significantly affecting the price.

Due to the fact that bigger liquidity pools result in less slippage and a better trading experience, several protocols, such as Balancer, began rewarding liquidity providers with additional tokens for giving liquidity to specific pools.

The ideas behind liquidity pools and automated market making are fairly basic, but incredibly powerful, since they eliminate the need for a centralized order book and the need on external market makers to provide liquidity to an exchange on a continuous basis.

Uniswap<sup>37</sup> utilizes the liquidity pools defined above, which are the most fundamental types of liquidity pools. Other experiments iterated on this principle and generated some intriguing concepts.

Everything comes with a risk, even more so in a very new and not regulated environment such as DeFi. Indeed, apart from the typical DeFi risks providing liquidity to a pool has two main risks: impermanent loss and liquidity pool hacks.

### 2.1.3 Constant product market maker and Impermanent Loss

Constant product market maker is the arithmetic formula which most Decentralised Exchangers rely on. Basically, every liquidity pool follows this simple equation:

$$x*y = k$$

where  $x$  and  $y$  are the quantity\*price of the specific tokens in the pool and  $k$  is a constant.

Assume for example a pool where:

$$x=50.000$$

$$y=50.000$$

$$k=2.5bn$$

Therefore, before the pool is open for trading both  $x$  and  $y$  are both priced at 1\$. When trading opens, users are allowed to exchange asset  $x$  for asset  $y$ , given that  $k$  must remain constant. Assume that user n°1 has 7.000  $x$  token which she wants to trade for  $y$  token, she would add her tokens to the pool which would reach 57.000  $x$  token. In order for the pool to keep the  $k$  value constant, it would give to user n°1 a number of  $y$  token equal to  $50.000 - (2.5bn / 57.000) = 6.140$ . This would keep the  $k$  value constant, indeed  $(50.000 - 6.140)*57.000=2.5bn$  resulting in the pool to have now 57.000 token  $x$  and 43.859 token  $y$ . The logic behind these set of rules is to increase the price of a given asset proportionally to demand for that asset and vice-versa, indeed, after the first trade the new prices of the two assets would be  $50.000/57.000 = 0.877\$$  for token  $x$  and  $50.000/43.859 = 1,14\$$ . Indeed, if we calculate again the constant with these new values we have  $(1,14*43.859)*(0,877*57.000) = 2.5bn$  (net of approximations).

The word "impermanent loss" refers to the momentary loss of cash that happens when providing liquidity. Often, it is characterized in terms of the contrast between holding and providing liquidity for an asset. Impermanent loss occurs most often in traditional liquidity pools when the liquidity provider (LP) is asked to

---

<sup>37</sup> <https://uniswap.org/>

supply two assets in the appropriate ratios and one of the assets is very volatile in contrast to the other, as for instance a Uniswap USDC/ETH 50/50 liquidity pool.

If the value of ETH grows, the pool must rely on arbitrageurs to guarantee that the pool price remains consistent with the real-world price in order to maintain the pool's value for both tokens. As a consequence, the liquidity provider basically loses money on the token's gain in value. If the LP withdraws liquidity within this time period, the impermanent loss becomes permanent.

To fully understand impermanent loss a concrete scenario is outlined below.

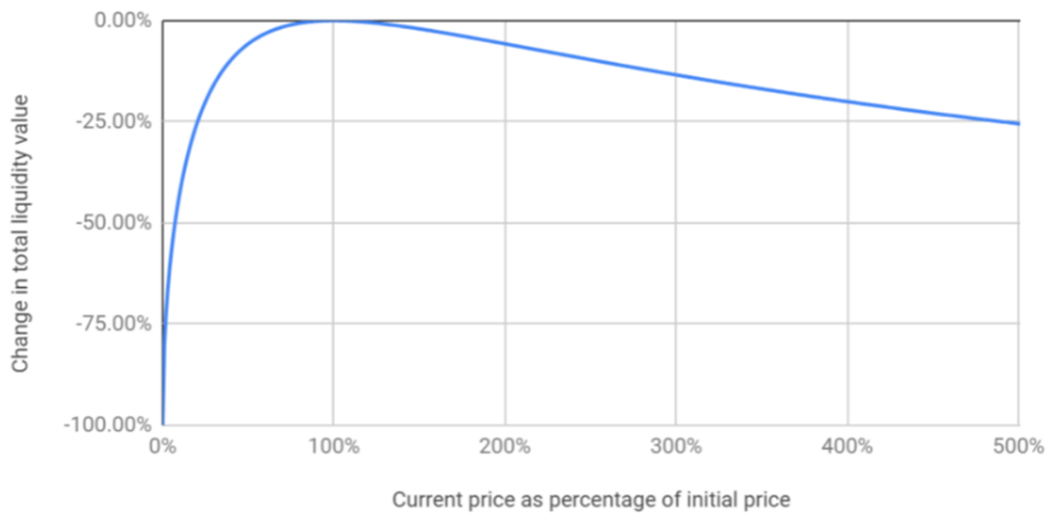
Assume a user provides liquidity to a USDC/ETH pool with a ratio of 50/50 and that ETH price is equal to \$100. Given that the liquidity provider provides liquidity for say 20.000\$ he would supply to the pool 100ETH and 10.000 USDC (which price always stays pegged to 1\$), indeed  $100\text{ETH} \times 100\$ + 10.000\text{USDC} \times 1\$ = 20.000\$$ . The amount of liquidity provided as well as the price of ETH are used as an example, the mechanics would work with any price and total amount of liquidity. Assume that the price of ETH rises in the global market, for instance, to \$110, this creates arbitrage opportunities for third party actors to buy ETH from the pool at \$100 and sell to other exchangers such as FTX for \$110. Entering the calculation described above the third party (arbitrageur) is able to buy 4,652 ETH for \$488 until the price of ETH reaches \$110 in the pool. The arbitrageur can sell his 4.652ETH to FTX for  $110 \times 4,652 = \$511.72$  resulting in a profit of  $\$511.72 - \$488 = \$23.82$ . On the opposite side, the liquidity provider is suffering impermanent loss, indeed, after this operation, in the pool there are 95,347 ETH and 10.488 USDC that are now worth  $(95,347 \times 110) + (10.488 \times 1) = \$20.976$ . Therefore, the liquidity provider, who has initially put \$20.000 worth of tokens into the pool has made  $\$20.976 - \$20.000 = \$976$  profit, but had he just hold the two coins without putting them into the pool he would have  $(\$110 \times 100) + (10.000 \times \$1) = \$21.000$ , hence he is suffering a impermanent loss equal to  $\$21.000 - \$20.976 = \$24$ .

Therefore, what is the incentive for liquidity providers to provide liquidity to a certain pool?

Without impermanent loss, the LPs would generate passive income via trading fees. For instance, in Uniswap, each transaction within a liquidity pool (es. Swap of USDC for ETH) incurs a 0.3 percent fee that is equally distributed among the pool's LPs.

Therefore, a Liquidity Provider, could keep earning passive income, even if incurring in temporary losses, because she will be rewarded with the 0.3% fees for the transaction processes by the pool in proportion to her portion of it (es if she provides 1.000\$ worth of ETH/USDC to a pool that has a total of 9.000\$ ETH/USDC she owns 10% of it and will receive the 10% of all the fees generated).

*Figure 6 - Losses to liquidity providers due to price variation compared to holding the original funds supplied*



*Source: Finematics (2021) <sup>38</sup>*

Additionally, some liquidity pools provide additional incentives to LPs via liquidity mining activities. Liquidity mining is a technique for providing LPs with more tokens in exchange for giving liquidity to certain pools or for using a protocol. In certain cases, the value of the additional tokens may completely compensate for the value lost due to impermanent loss, making liquidity supply very useful.

## 2.2 Traceability

Consumers, business partners and regulators are increasingly demanding transparency. Organizations struggle to provide the data due to the lack of connectivity between the networks of the supply chain. This leads to highly manual efforts and reconciliation activities which are often outsourced and exposes data to third parties. Moreover, it is increasingly strategic to improve tracking and visibility of qualitative and sustainable activities and parameters.

Blockchain can help organizations to transform so they can give consumers, business partners and regulators the transparency they demand in ways that create lasting business value. Blockchain Traceability solutions provides a trusted platform for traceability and transparency within an ecosystem through the use of Notarization and Tokenization. This technology can help businesses deliver long-term value by improving brand equity, sustainability and revenues.

In this sub-chapter will be analysed three different use cases of business that have adopted the technology to their supply chain, namely Blockchain Wine Pte. Ltd. (with the platform TATTOO Wine), Carrefour and

<sup>38</sup> <https://finematics.com/impermanent-loss-explained/>

ANSA, these are just a small portion of the business adopting the technology to improve their processes and deliver higher transparency to their consumers.

Even as the enthusiasm around the usage of blockchain-based traceability has grown, it is critical to remember that many of these applications are still in their infancy. The following chapter provides a thorough understanding of the technological foundations of blockchain traceability, additionally, a summary of the many uses of blockchain traceability in various areas is outlined, with a focus on the solutions that EY has developed in this field for different clients.

### **2.2.1 Food & Beverage**

Organic food purchasers want quality and rely on certifying bodies to certify the goods' quality and give information about the products' origin. However, with regards to organic food traceability, various complications arise, including questions about organic labelling, certification fraud, and worries about food information openness.

Digitizing manual procedures and installing a Blockchain-based traceability system may be seen as a potential option for a more stable and trustworthy food supply chain<sup>39</sup>. Information regarding food sources is especially significant in the organic food supply chain since it may show pesticide usage, genetically modified organisms, environmental or carbon impact, and other critical information.

Due to the fact that blockchain intends to keep an exhaustive record of food items' itineraries from source to consumption, it contributes in the avoidance of food safety crises. Everyone in the supply chain, including supply chain associates, import regulators, and food safety inspectors, has real-time access to data. And, perhaps most importantly, data saved on Blockchain is completely trustworthy since it is immutable and cannot be altered or fabricated at any point in time.

Another benefit of Blockchain is that it aids in the development of customer confidence when it comes to getting organic goods.

Today's buyers strive to make purchases that are both healthy and environmentally responsible<sup>40</sup>. Many individuals are now willing to pay a premium for healthier versions of their favourite meals and beverages. However, how can they be certain they are obtaining 100% original goods? Due to Blockchain's total decentralization, it may be used to explain a product's narrative to the buyer, even at the point of purchase, demonstrating whether the product is organic or not and so establishing consumer confidence.

---

<sup>39</sup> <https://www.undp.org/publications/blockchain-agri-food-traceability>

<sup>40</sup> Blockchain for Agrifood traceability, UNDP, 2021.



While blockchain has the potential to reshape the food supply chain sector, there are still significant limitations to consider.

Adoption is one of the primary hurdles in using Blockchain to improve traceability. To be effective, Blockchain requires involvement from all parties and points of contact. Additionally, data validation in a blockchain system is a concern, since food branded organic or fair trade may be non-compliant. Additionally, data integrity remains a concern, since it is in the hands of data collectors.

## **TATTOO WINE**

The necessity for a wine supply chain traceability system is critical since counterfeiting and the overuse of preservatives and dangerous chemicals have increased. To address these issues, the wine business requires not just a system that allows consumers to check the 'ingredients' and composition of each batch of wine from grape farmers to merchants, but also one that caters to the fine wine sector. However, existing systems (for wine supply chain management) are RFID and web-based, making it easy to forge stored data as needed and providing no integrity. Rather than that, winemakers today check and certify wines via the use of paper records and physical certificates. A few unique components on records or certificates, such as stamps and signatures, are intended to deter wine fraud and assist authenticators in determining the wine's provenance.

Fine wine has long been purchased and sold on the basis of a high degree of confidence; indeed, bottles are sold based on statements about their origins, ages, and how particular storage conditions were satisfied. Customers, on the other hand, spend hundreds or even thousands of euros for selected bottles, but fraudsters can easily copy signatures and sell counterfeit bottles. Additionally, clients lack insights into the supply chain and into all the necessary processes for a particular sort of wine. The solution is a blockchain-based system for tracing the wine supply chain, in which each transaction is logged as a block in the chain and accessible to all relevant players.

These data blocks are immutable since any modification to the recorded data invalidate the followings. Along with offering a foundation for quality information management, the proposed traceability system would promote openness, accountability, safety, and security across the whole process, from the raw material to the bottle or, in the case of the fine wine industry, from one client to another. To certify the "made in" of a particular bottle of wine using a blockchain-based traceability system is an example of a digital relationship between the producer and the final customer, who, via a smart label on the wine bottle, can read about the wine producer (identified by a digital signature), the entire process of wine cultivation, production, and processing, thereby increasing the consumer's trust. This procedure is enabled by blockchain technology, which records all information about a product, allowing the customer to verify its origin, attributes, and whole

manufacturing process at any moment by scanning the QR Code printed on the wine label with his or her own smartphone.

The current model of quality wine distribution is complex and requires numerous steps along the supply chain. Consumers can choose only a few labels from companies that reach the critical mass needed to export their products and find the right channels, with prices much higher than those applied at source. In this context, consumers have no guarantee of the authenticity of the wine regarding country of origin and production.

All these factors become an untapped opportunity for producing countries to increase exports both in relation to the growth of the market in some countries, for instance China and in terms of market share, also through communication and storytelling and with an optimisation of the distribution chain, which today is long and complex.

EY developed a marketplace for TATTOO Wine which allows consumers to buy premium wines through a secure, blockchain-based platform enabled by digital tokens to track origin, quality and authenticity of new and vintage wines, removing layers of middlemen enabling cost efficiency<sup>41</sup>. The platform currently offers selections from wineries in France, Italy, Spain, Australia, New Zealand, the Americas and plans to help wineries of all sizes worldwide to expand into the Asia Pacific market<sup>42</sup>.

TATTOO allows wineries to register products history on Ethereum's public blockchain and represent them as assets on Quorum permissioned blockchain. The unique and non-replicable identification of the products is guaranteed by the use of tokens combined with 3D QRcodes, obtained through a random application of colour stains around a two-dimensional QRcode, this prevents the counterfeiting of the code.

In fact, tokens (bottles uniquely linked to the production lots registered on Ethereum) are exchanged for fungible tokens (TATTOO Token) representing the payment made with fiat currency. Each purchase made on the platform is a reward generated and distributed among those who have TATTOO Token in their wallet. Wines and shipments are then tracked to show the consumer the distribution steps, thanks to the integration with FedEx systems.

TATTOO is based on the EY OpsChain platform while users will access through a user friendly experience distributed on the SAP® Commerce solution.

EY has developed a European wine market research in Asia and an expansion strategy in the markets of China, Japan, South Korea, Thailand and Singapore, where European wine consumption is increasing. EY through OpsChain Traceability has provided digital tokens and smart contracts used to represent the entire life cycle

---

<sup>41</sup> [https://www.ey.com/en\\_gl/news/2019/11/ey-blockchain-platform-supports-blockchain-wine-ptltd-to-launch-tattoo-wine-marketplace-across-asia-pacific](https://www.ey.com/en_gl/news/2019/11/ey-blockchain-platform-supports-blockchain-wine-ptltd-to-launch-tattoo-wine-marketplace-across-asia-pacific)

<sup>42</sup> <https://www.digitalvoice.it/blockchain-tattoo-wine-prima-piattaforma-e-commerce-del-vino-per-il-mercato-cinese/>

of a specific bottle of wine, ensuring its provenance and distribution efficiency. The goal of the platform is to enable a Wine token economy for the purchase of wine and to create a real industry token enabling B2B sales and value-added services (i.e. insurances, warehousing, etc.).

The TATTOO Wine platform is the first global e-commerce platform that uses blockchain technology to facilitate wine trading and provides authenticity and traceability features for consumers and wine merchants. It is based in Singapore and serves also as a forum for reviews, ratings, opinions and recommendations on wine pairings.

EY was responsible for the design and development of the entire solution consisting of:

- OpsChain traceability module with public Blockchain
- Blockchain permissioned by Quorum
- eCommerce based on SAP Hybris technology

The platform has been released on 1st November 2019.

Technologies involved (hardware, software and tools) are:

1. Scalability of the solution for a consumer target of over 5,000,000 customers
2. Ethereum blockchain
3. Quorum blockchain
4. Microsoft Azure
5. SAP Hybris
6. Interoperability between TATTOO Wine reporting/ management systems and FedEx systems
7. Tokens standards ERC20 and ERC721
8. Security by design

## **Carrefour**

Growing international competition is leading to price pressure in key markets while increasing demand for private labels provides an opportunity to grow margins. The "Food First" strategy – non-food products secondary – with a particular focus on freshness, led the organization to innovate to be consistent with the new habits of modern consumers, who are increasingly attentive to the quality and healthiness of food products, and search for new solutions to accelerate the internationalization process. The client asked EY to support them in supply chain integration to guarantee and improve the traceability of private label product provided by suppliers, to implement automatic Q&A checks and full auditing, and to communicate the quality of the

production process to customers. Carrefour Italia will be one of the first sub-holdings (along with Italy and Brazil) to be consistent with the French subsidiary's holding investment in blockchain technology for supply chain integration.

EY applied the solution “EY OpsChain Traceability” - the first blockchain software developed to certify the origin and the attributes of a food and beverage-related product, able to track the entire supply chain and report any alteration or contamination of the product; this currently applies to the following categories of products: fish products, cheese, wine, organic food products and frozen products; nevertheless, it shows high replicability potentials in this sector that are currently under exploration by the EY blockchain hub<sup>43</sup>.

Mechanics:

Consider chicken meat as an example.

1. Incubation: In a hatchery, the chick is born.
2. Breeding: four individuals enter the relevant data into a dashboard, which is directly connected with the blockchain, this means that this data is notarized and associated to this specific "raw material".

The first is the breeder, who specifies when the chicks arrived at his house and were then transported to the slaughterhouse. The second is the feed mill, which provides information about the composition of the batches delivered to farmers as well as the absence of GMOs. The third party is the veterinarian, who certifies that no antibiotics were prescribed. The fourth is the company Certipaq, which verifies the brand's authenticity.

3. Slaughtering and processing: the slaughterhouse, which is also responsible for the packaging, indicates the id, lot number, and day of departure to the Carrefour warehouse.
4. Distribution: the warehouse records the date of arrival of the lots as well as the date of arrival and date of delivery to the stores, as well as the characteristics of the environment through which the product transits.

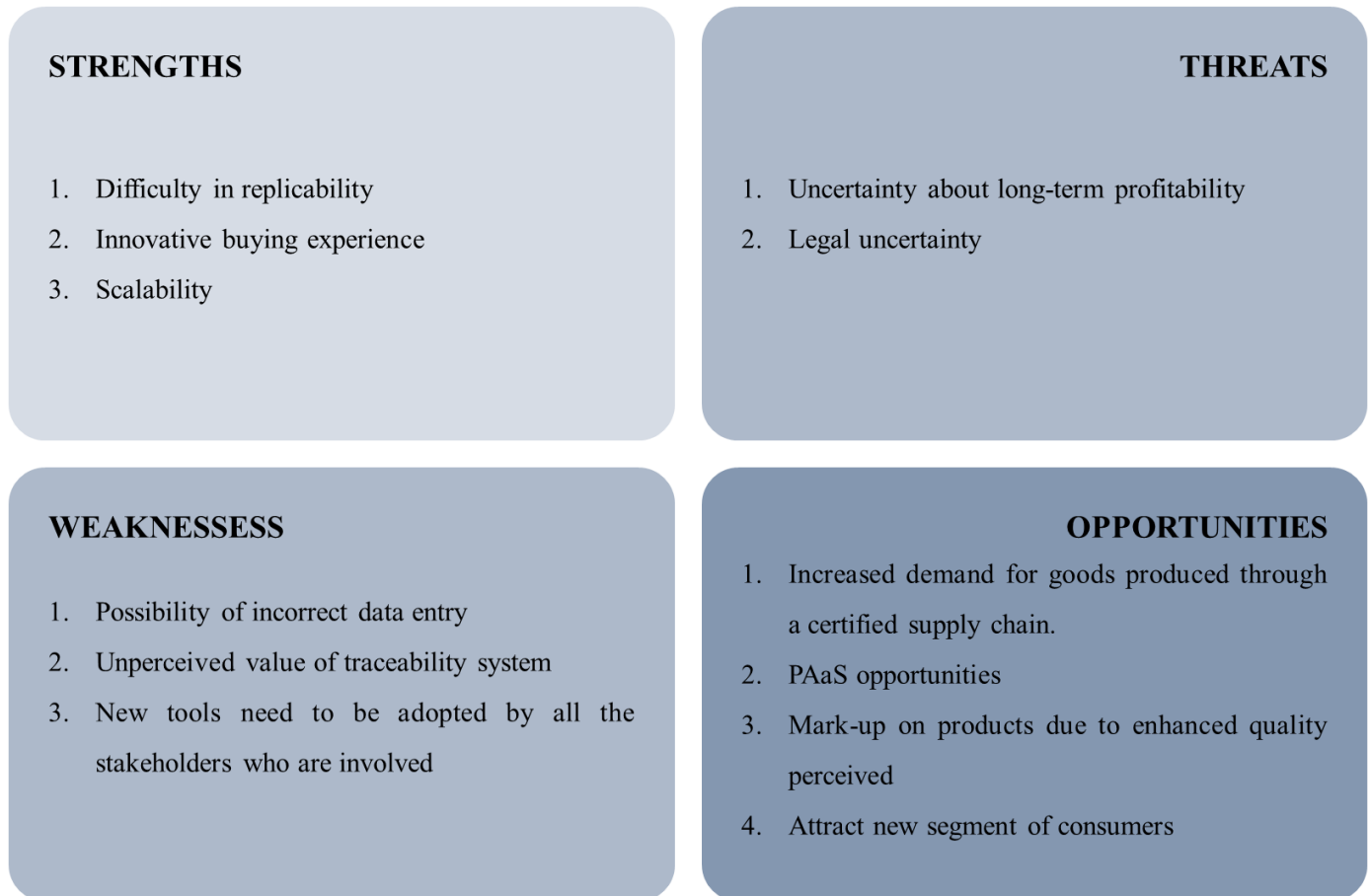
The blockchain-certified products, such as chicken, tomatoes, and potatoes, are provided with a QR code printed on the outside of the package. By scanning this QR code, the customer is directed to an independent platform where they can access information about the supply chain, such as the specifications of the products used for processing, the date and location of the same, and the storage that preceded the sale.

## **SWOT ANALYSIS OF THE SOLUTION**

---

<sup>43</sup> <https://coinidol.com/carrefour-italy-tracks-food-using-blockchain/>

*Figure 7- SWOT analysis of Carrefour traceability solution*



**Strengths:**

1. Carrefour has the potential to be a pioneer in Europe since the project is difficult to replicate because the retailer is also equipped with its own production line of fresh food goods under the Carrefour brand, which is a unique and independent independent brand in Europe.
2. Innovative buying experience.
3. Scalability: as mentioned above the solution can scale to all Carrefour products.

**Opportunities**

1. Increased demand for goods produced through a controlled and certified supply chain.
2. Offer the platform as a service to other brands within or even outside Carrefour existing stakeholders and partners.
3. Add a mark-up on products due to enhanced quality perceived.
4. Attract the segment of consumers who were reluctant to buy due to poor traceability control opportunities.

## Weaknesses

1. The possibility of incorrect data entry exists as long as the platform is not equipped with a system of smart sensors that are directly connected to it. This is especially true upstream in the manufacturing process.
2. Blockchain is an emerging technology, therefore customers may not fully understand the potential of it hence losing the perceived value of the traceability system.
3. All the stakeholder within the value chain need to adopt new tools or sometimes even change existing processes in order to enable the solution to work.

## Threats

1. As a result of Carrefour's innovation-driven strategy, there is some uncertainty about the long-term profitability of the company's new product launch. In fact, in technologically advanced industries, given the elevated potential for improvement of a new technology compared to a previous technology, there is the possibility that the former, depending on how revolutionary the project is, will be rendered obsolete by new platforms in a relatively short period of time.
2. Legal uncertainty: at the moment, the blockchain does not have any legal significance, owing to the fact that it has only recently begun to be included in the majority of European Union regulations and directives. As a first step, the government intends to research the issue in order to identify technical standards that will be able to certify its legitimacy. To date, there has been no quantification of the timeframes required to complete the process.

### 2.2.2 News & journals

The exponential expansion of unreliable information and the proliferation of so-called "fake news" poses a severe challenge to media firms' credibility. The impact of fake news has exploded in recent years as the media landscape has been transformed by the internet, and the effects of these threats are frequently amplified by algorithms that are aimed at providing users content they are interested in, which also means they generally tend to believe it when they read it.

The Agenzia Nazionale Stampa Associata (ANSA) has developed, in collaboration with EY a solution for the verification of the provenance of a given news. ANSA was facing a challenge of trust due to the high number of third parties copying its news and altering them for many reasons, as for instance increase click-through rates, conversion rates etc.

Therefore, ANSA developed ANSAcheck, ANSAcheck is a news certification system powered by blockchain technology that ANSA has chosen to tighten control over the flow of its news, ensuring that they cannot be used or disseminated in an untruthful or inappropriate manner, while also guaranteeing readers the source's highest quality and reliability<sup>44</sup>.

By using the “stamp” at the end of an ANSA news item or "ANSA source," it will be able to:

1. Verify the history and credibility of a news item by referring to the main source.
2. Allow for comparisons between the news read and the ANSA source.
3. By improving public trust, enable editors, agencies, and media to qualify as quality news producers.

On a technical level the solution consists of four main steps:

1. When the news is created by ANSA, the Blockchain records its identifier so that its future events can be tracked and an hash of the content of the news is created.
2. When the news is modified or updated by ANSA, the Blockchain records the event allowing transparent versioning.
3. When the news is resumed by the Publishers participating in the initiative, the Blockchain verifies the authenticity of the news recorded by ANSA and records the resumption event enabling future consultations of the news resumed by the publisher thanks to the ANSAcheck stamp.
4. When the end-users want to verify the reliability of the news they can click on the ANSAcheck button on the end of the page, see the hash of the news as well as the notarisation transaction happened on the Blockchain.

---

<sup>44</sup> [https://www.ansa.it/sito/static/ansa\\_check.html](https://www.ansa.it/sito/static/ansa_check.html)

*Figure 8 - ANSAcheck button*

Nella piattaforma ICoGen **"13 casi confermati in Italia di variante Omicron del Sars-CoV-2: 7 del cluster in Campania; 3 in Veneto; 1 rispettivamente in Piemonte, Sardegna e Bolzano. Del totale dei 13 casi, 12 sono importati o contatti di importati. Per uno (in Veneto) sono in corso indagini. In corso anche il sequenziamento di altri 4 sospetti"**. Lo riferisce l'Istituto superiore di sanità.

**"La variante di Omicron per ora è stata segnalata in 57 paesi** e prevediamo che il numero continuerà a crescere. Alcune caratteristiche di Omicron, tra cui la sua diffusione globale e il gran numero di mutazioni, suggeriscono che potrebbe avere un impatto importante sul corso della pandemia". Lo detto il capo dell'Oms Tedros Ghebreyesus nel briefing sul Covid da Ginevra.


RIPRODUZIONE RISERVATA © Copyright ANSA



*Source: Ansa (2021)*



Figure 9 - Info about News ID and News Hash

 **ANSAcheck**  
Notizia d'origine certificata

**++ Omicron:neutralizzata da 3 dosi vaccino Pfizer/BionTech ++**

Rilasciata il  
08/12/2021 13:42

ID News  
699e4c407b6fdd1898f987e88444336a

Hash Contenuto  
6710a6986f72c19488b8c42784adb953 (MD5) ↕


**La storia di questa notizia**

1

 Notizia registrata da ANSA il 08/12/2021 alle 13:43

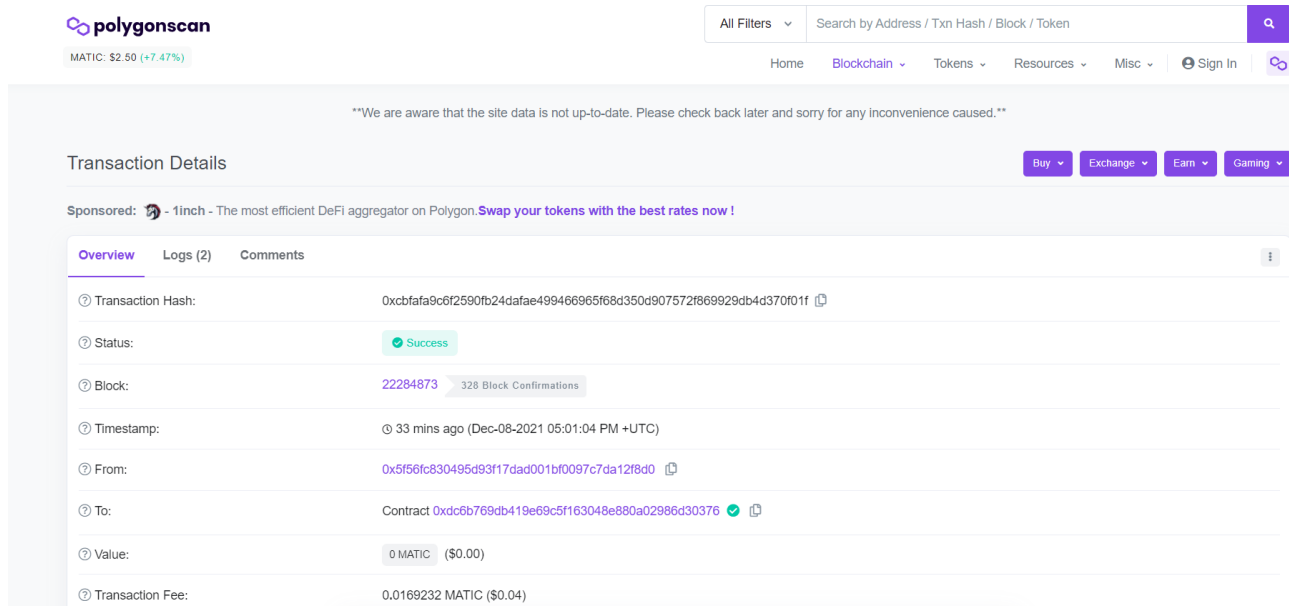
Registrata nel blocco **AC202112081700**

**CERTIFICATO ANSACHECK**

 INFO SU ANSACHECK

Source: Ansa (2021)

Figure 10 - Visualization of the transaction on the Blockchain



Source: Polygonscan (2021)

A further analysis of this Blockchain use case finds 3 main benefits for ANSA to have adopted such solution:

1. Enable ANSA and its main clients to establish themselves as a quality supplier by fostering public trust.
2. Bridge the divide between journalism and the publishing ecosystem's participants.
3. Develop new business logics and models (reputation system, as-a-Service replicable solution, etc.).

The initiative's objective was to provide an innovative solution for the traceability of news in the publishing and journalism industries via the use of blockchain technology and its inherent properties of immutability, transparency, and security. The purpose of this project is to follow the tale of ANSA-published news that is disseminated to its clients or is reported by other parties (agencies, news outlets) with attribution to the ANSA source. The suggested approach sought to distinguish ANSA news from those of other news suppliers. By using blockchain to monitor the news narrative, ANSA could solidify its brand and publications may join a trustworthy ecosystem and profit from its reputation. ANSA will therefore preserve his trusted brand by preventing it from being associated with false news and will also be able to track the quantity of news articles reposted by other providers. ANSA is therefore the world's first news organization to establish a true public Blockchain-based news management system.

## 2.3 Auditing and Accounting

To increase efficiency and effectiveness, businesses need continual communication and exchange of information. There is a trade-off between openness and privacy: the more information provided, the more transparent the business becomes, but at the risk of sacrificing personal and sensitive information.

Blockchain technology is one of the most disruptive new technologies in auditing and accounting; while the development and research of blockchain applications by audit companies remain in their infancy, they may one day increase the audit's quality, efficiency, and efficacy. Integration of accounting on blockchain reveals the potential for streamlining unnecessary operations, increasing transaction settlement speed, and preventing financial report fraud. Additionally, it will be capable of influencing corporate governance procedures.

The society relies on auditors to build trust in certified financial information and to assist the capital markets system in operating more confidently. Auditors operate under stringent regulatory frameworks, professional codes of conduct, and international standards, and are completely independent from the organizations they audit. They use impartiality and judgement to give reasonable confidence about the accuracy of an entity's financial statements and, according to the involvement, about the effectiveness of a company's internal controls over financial reporting. An audit is a process that verifies that the evidence supporting recorded transactions is appropriate, credible, unbiased, precise, and verifiable. Acceptance of a transaction into a reputable blockchain may provide enough audit proof for some financial statement claims, such as the transaction's existence.

As an example, when a bitcoin transaction is made to purchase a product, the transference of bitcoin is added to the blockchain. But by just reviewing information on the Bitcoin blockchain, an auditor still might not be able to identify what goods was really provided to customers.

As a result, depending on the type of the transaction, documenting a transaction in a blockchain might also not offer sufficient acceptable audit proof. This means that even after being recorded on a blockchain, a transaction might still be:

- unlawful, false, or illegal;
- performed by related entities;
- tied to an arrangement "off-chain;"
- categorized improperly in financial reports.

As an additional point of interest, many transactions reflected in the financial accounts show projected values that vary from the historical cost. Even though the underlying data are entered in a blockchain, auditors will still be required to assess and execute audit procedures on management's estimations.

Audit data may be obtained from central places as a result of widespread blockchain usage, and auditors may build techniques to collect audit evidence straight from blockchains as a result of widespread implementation.

While performing audits upon these transactions, the auditor must take into consideration that the information may be wrong as a result of human mistake or fraud. Since a blockchain is not likely to be controlled by the business being audited, this will raise new issues for the auditor. A blockchain audit will need the auditor to retrieve information from the blockchain and determine whether or not the data is trustworthy. It may also be necessary for the auditor to comprehend and evaluate the dependability of the consensus process for the individual blockchain under consideration. In this evaluation, it may be necessary to take into account the possibility that the procedure may be modified. Auditors do have to be aware of the possible effect that the use of private or public blockchains has on their audits as a new source of knowledge for the accounting records when more businesses investigate the use of private or public blockchains.

Aside from that, they will need to assess management's accounting procedures for digitized assets and liabilities, that are not yet covered directly by accounting standards or accepted accounting principles. They will have to think about how to customize audit processes to take advantage of the strengths of blockchain technology while also addressing new concerns.

Because financial data and business sensitive data are being exposed on public blockchain, organizations will be more inclined to choose a private blockchain, where only approved parties are able to access and read records, or to generate new transactions, for example. Businesses have a number of issues, one of which is that a private blockchain would provide less transparency on data while also excluding the general public, thereby limiting the anti-manipulation capability.

In order to compile the accounting records required for establishing the annual management outcome for a firm, blockchain technology can ensure that data is collected and notarized in a safe and certified manner. This could be done in a way as to make the accounting records inalterable, then make them impasse so that they are not subject to Accruals Earning Management, to eliminate the need for auditors, and to control transfers between related entities. Due to the fact that is tagged with a tamperproof time stamp, data would permanently be stored using this accounting approach, and thus impossible to be modified once it has been recorded.

Furthermore, blockchain has the potential to revolutionize interactions between businesses and with external parties such as auditors, financial institutions, tax authorities and courts as well as with the government and other public-private partnerships (PPPs). Through the use of the distributed information ledger, it is feasible to encourage data sharing in a safe way while also being able to trace which individuals have access and revoke their access in the case of conduct that is not deemed proper by the data owner.

The blockchain allows real-time accounting data collecting. In the existing system, real-time data gathering is prohibitively expensive due to high costs of performing numerous highly time-consuming activities, including the collection of the data itself and the following internal audit of the process for validating the platform's operation.

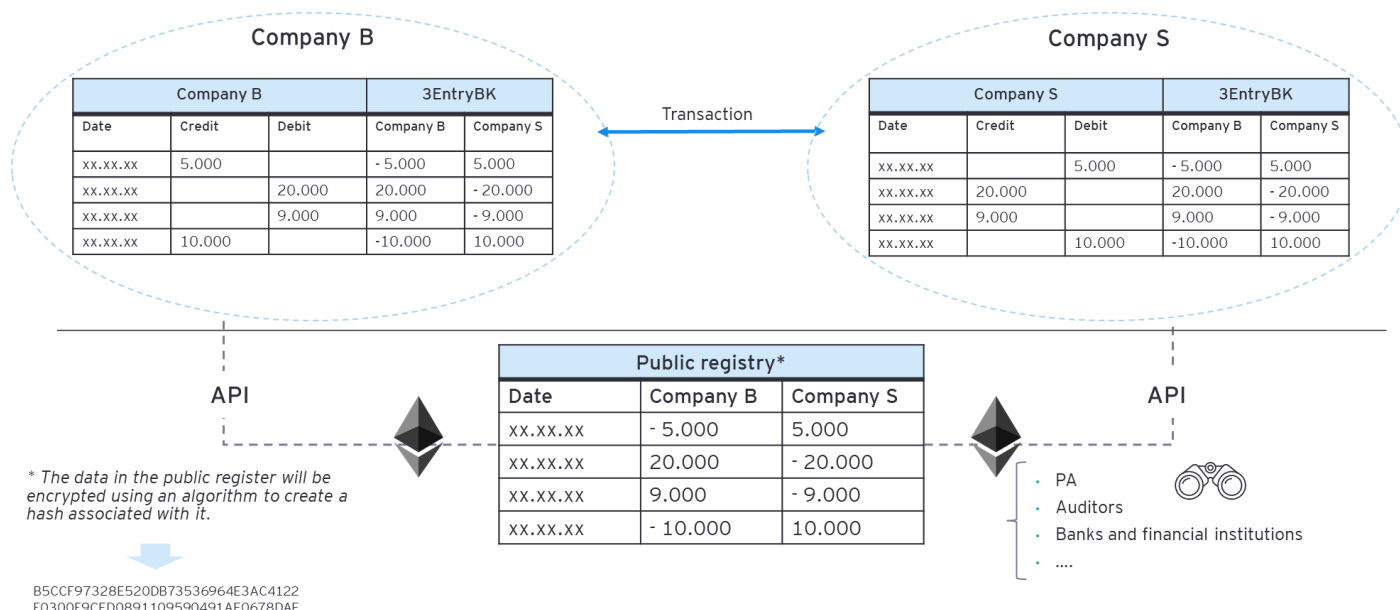
### **2.3.1 Triple entry accounting**

Through the use of blockchain technology to handle the company's accounting data, a shift from a double entry system to a triple entry system would indeed be made. The existing system, which is built on a double entry method, necessitates the use of a double book entry form for the two components of the same transaction. Thus, each party would be required to create its own book entry form autonomously of the other, which, in addition to resulting in duplication of bookings, may result in performing various errors as for instance the formation of discrepancies between the two distinct accounting records, inaccuracies, and, additionally, it necessitates a correspondence among the two parties' records following reconciliations.

Take into account a buying products transaction in which company B (buyer) purchases an item from company S (seller), who will generate an invoice at the time of purchase. In a double entry system, this results in the need to perform two series of pair and opposite book entries. Company B will first create bookings for the buying and the subsequent creation of debt; subsequent to payment, the buyer will create bookings for a movement that will eliminate the debt and result in a cash flow to the supplier. Company S, on the other hand, will need to make its own bookings, first for the release of the sale item from the company in exchange for the creation of a credit with the buyer, and then for a financial movement associated with the elimination of the credit-related item and the emergence of cash-in-flow. By implementing a triple entry model on a blockchain, it would be feasible to increase the system's efficacy and efficiency. Among the network's many participants, the triple entry system would produce a unique shared ledger in which all transactional information would be stored. A single public ledger enables automatic updating via a single book entry and enables communication and availability to all counterparts. Assume the identical financial transaction mentioned above between the two companies, this time, each actor will have two distinct entries, one pertaining to the acquisition/sale of the item and another pertaining to the payment. Company S would produce and sign a transaction comprising the purchase data at the moment of sale to company B. When signed by both parties, the event will be put in the distributed ledger, where it may be audited. The buyer would be obligated to pay the seller an amount in exchange for the commodity X upon inscription in the public ledger. The smart contract would control the relationship between the two parties by temporarily rendering the funds specified by the purchaser ineligible for use as security by the debtor. At the moment of delivery, the smart contract would release and transfer the cash to the seller, rendering the debt uncollectible. Information is

encrypted and subsequently rendered immutable in this system, making it difficult to forge or erase registered information.

*Figure 11 - Triple entry book-keeping model*



To ensure the proper operation of a triple-entry model, three distinct levels with distinct but complimentary functions are required:

- **Standards and Reports:** based on the XBRL39<sup>45</sup> global system; by using the same language, it enables the easy extraction of data by auditors and accountants.
- **Data Consistency and Reliability:** it may be implemented on a variety of public and private blockchains. It ensures the integrity of data and certifies its security throughout storage and transmission.
- **Data Storage and Distribution:** having the data conforming to universal standards and secure and comprehensive, data is stored in decentralized storage, as for instance IPFS<sup>46</sup>, securing data and its privacy.

## 2.4 Digital identity

Self-sovereign identity—abbreviated SSI—is a new paradigm for digital identification on the internet, i.e., how we develop trusted connections with websites, services, and applications with whom we need to establish trusted relationships in order to access or secure private information. SSI is a paradigm change in digital

<sup>45</sup> XBRL is the open international standard for digital business reporting

<sup>46</sup> The InterPlanetary File System (IPFS) is a peer-to-peer network for storing and sharing data in a distributed file system

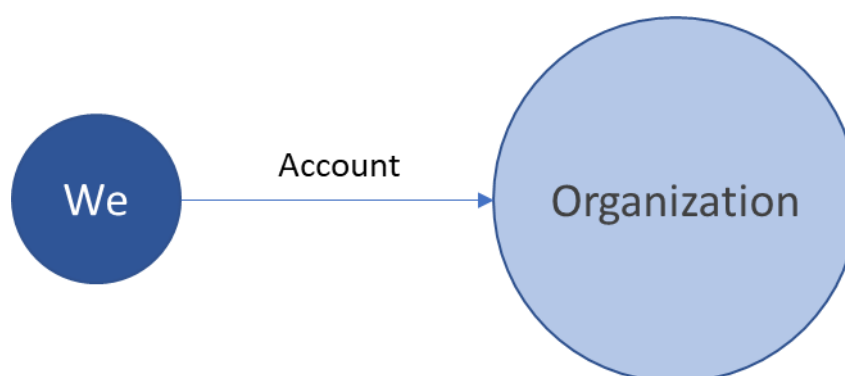
identity, driven by new technologies and standards in encryption, distributed networks, cloud computing, and smartphones.

In order to understand the aforementioned paradigm shift, it is important to understand the three model of digital identity: centralized model, federated model and finally the decentralized identity model.

The first model, the **centralized model**, is the most straightforward to comprehend. It is the approach we have historically used for almost all IDs and credentials, including government-issued identification numbers, passports, identity cards, driver's licenses, invoices, Facebook and Google logins. These are all issued by central governments or service providers such as banks, telecommunications corporations or tech companies. Additionally, the centralized model is the original form of online identity—and the one that we continue to utilize in many circumstances today. We create an identity by registering for a website, service, or application and creating an account (usually a username and password). As a result, the paradigm is sometimes referred to as account-based identification. In a world of centralized identification, our identity (or identification) does not exist without a centralized account. The authenticated "we" is granted authorization to integrate with a website, service, or application because a given organization provides us with credentials that represent us but have restricted limitations and rights. All in all, the given organization owns those credentials. If we remove all of your accounts with these centralized providers, we will lose access to services. Yet all the data about us would still belong to the organization, outside of our control. The locus of control on a restricted number of corporations to provide our identification on the internet, is one of the main problems, among others:

- We are solely responsible for remembering and keeping all of our usernames and passwords (and, in certain situations, additional multi-factor authentication techniques such as one-time codes).
- These centralized databases of personal information act as massive honeypots, resulting in some of the most serious data breaches in history.

*Figure 12 - Relationship between us and organization under the account-based identity model of the internet*



The **federated identity model**, mitigates some of the pain points of the centralized model by adding a “middle-man”, an identity provider (IDP). Today, we may have a single identity account with the IDP, which can log us in and exchange certain basic identity data with just about any site, service, or application that makes use of the IDP. A federation is the gathering of all sites that utilize the same IDP (or set of IDPs). Inside a federation, each organization is sometimes referred to as a relying party (RP). From 2005, three generations of federated identification protocols have been developed: Security Assertion Markup Language (SAML), OAuth, and OpenID Connect, each of which has achieved some kind of success. Single sign-on (SSO) is currently a typical feature of the majority of business intranets and extranets when these protocols are used.

Federated identity management (FIM) began to gain popularity on the consumer internet, where it was labelled user-centric identity. Using OpenID Connect protocols, social login buttons have become a regular feature on a large number of consumer-facing websites.

*Figure 13 - Social login buttons*



Despite the fact that federated identification has been in development since 2005, it has yet to provide the internet's missing identity layer. Several considerations exist:

- There is no universally compatible IDP. As a result, consumers need many IDP accounts, and quickly forget which IDP they connected with whatever site, service, or application.
- IDPs must adhere to "lowest common denominator" security and privacy regulations because of the large number of sites they must service.
- Many users are concerned with the idea of a "man in the middle" overseeing all their interactions, monitoring a user's login behavior across several sites.

Large IDPs are some of the most fertile ground for cybercrime. Accounts associated with IDPs are not more portable than accounts associated with centralized identities. When we quit an IDP such as LinkedIn, Facebook, or Instagram, we lose access to all of our accounts.

Due to security and privacy issues, IDPs are unable to assist consumers in safely sharing some of their most important personal information, including passports, government IDs, health data, and financial data.



In 2015, a new model, the **decentralized identity model**, influenced by blockchain technology made its debut. This concept was essentially decentralized and did not rely on either centralized or federated identity suppliers. It developed at an incredible rate, including advances in encryption, distributed systems, and decentralized networks. It stimulated the development of new decentralized identification standards such as verifiable credentials (VCs) and decentralized identifiers (DIDs),

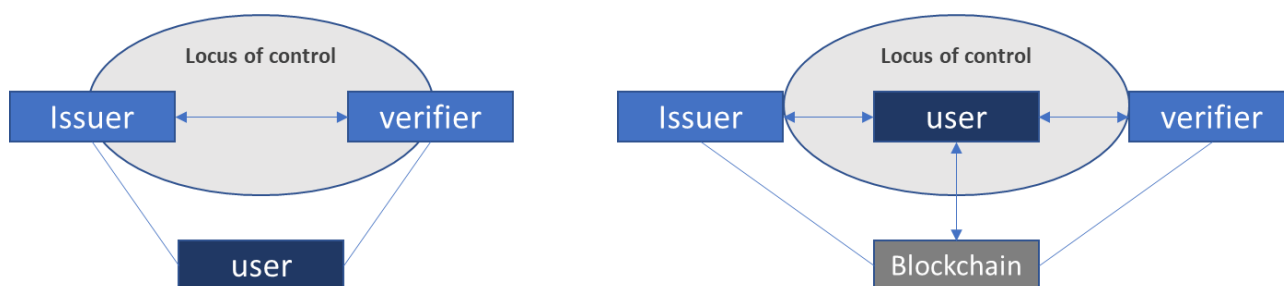
However, the most significant distinction between this model and the previous one is that it is no longer account-based. Rather than that, it operates similarly to how identification works in the actual world: it is founded on a direct interaction between an individual and another party as peers. Neither one of them "offers," "oversights" or "owns" the other's connection. This is true regardless of whether the opposing party is an individual, an institution, or an object. Neither party has a "account" with each other in a peer-to-peer connection.

Peer-to-peer interactions are naturally decentralized, since each peer may connect to any peer in any location exactly how the internet operates. However, how does this create a layer of identity? And why is blockchain technology required?

The solution is public/private key cryptography: a method of safeguarding data using mathematical methods based on each party's cryptographic keys. Rather of leveraging blockchain technology to create and send/receive bitcoin, identity management leverages it to create a decentralized public key infrastructure (DPKI). In essence, blockchain as well as other decentralized network technologies can provide a robust, decentralized solution for exchanging public keys directly between peers to establish private, secure connections and recording some of these public keys on public blockchains to prove the signatures on digital identity credentials (verifiable credentials) that peers can exchange to establish proof of real-world identity.

All in all, why is self sovereign identity (SSI) so important? Because it represents a shift in the locus of control, putting the citizen/user at the centre of it by decentralizing the structure. The locus of control in centralized and federated identity models is with the network's issuers and verifiers. The focus of control changes to the individual user in the decentralized SSI identity paradigm, who may now engage with everyone else as a complete peer.

*Figure 14 - The shift from centralized/federated identity model to Self Sovereign Identity*



As in the other two models there are three main actors: issuer, user and verifier. The issuer is the entity that issues the identity to the user (in SSI this is done in the form of a verifiable credential), the user is the one that receives and uses his digital identity to authenticate himself with the verifier once he needs to access a determined service. In the SSI model there needs to be added a few more elements: Decentralized Identifiers (DIDs), Verifiable Credentials and of course Blockchain. DIDs<sup>47</sup> are a new kind of identifier that provides verified, decentralized digital identification. A DID is a unique identifier for any subject (e.g., a person, organization, item) as specified by the DID's controller. In contrast to traditional federated identifiers, DIDs are detached from centralized registries, identity providers, and certificate authorities. While other parties may be enlisted to assist in the finding of information about a DID, the design permits the DID's controller to establish authority over it without obtaining permission from any other person. Credentials are an integral part of our everyday lives; driver's licenses attest to our ability to operate a motor vehicle, university degrees attest to our level of education, and government-issued passports attest to our ability to travel between nations. The standard<sup>48</sup> of Verifiable Credentials (VC) defines a system for expressing various types of credentials on the Web in a safe, privacy-preserving, and machine-verifiable manner.

Both DIDs and Verifiable Credentials are standards created by the W3C, the World Wide Web Consortium, the main international standards organization for the World Wide Web.

Below we can find the framework<sup>49</sup> for a self sovereign identity model. To summarize it, as in the physical world we have the holder (citizen) who requests a credential to a given issuer (es. The municipality), the issuer issues the requested credential, signs it and anchors a proof on the Blockchain. The holder receives the credential and stores it in his wallet (digital wallets come in the form of apps), then, when he needs to access a given service he is asked by the verifier to identify himself by sharing his identity credential (or any other

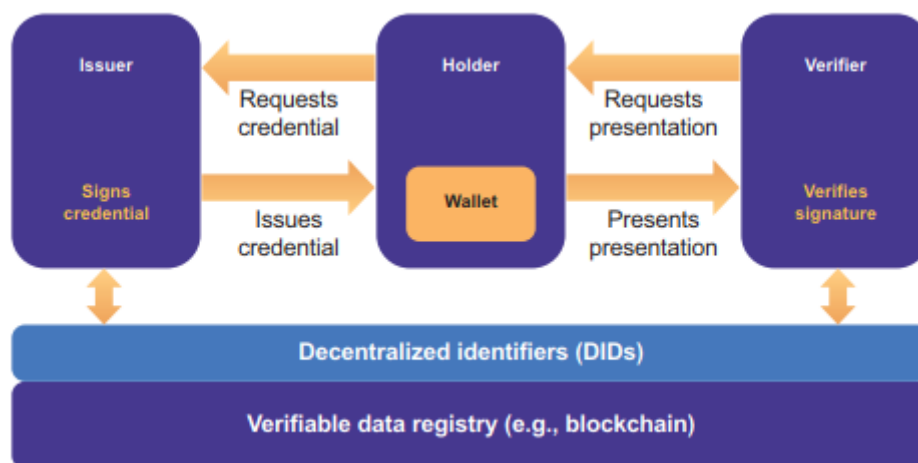
<sup>47</sup> [www.w3.org/TR/did-core/](http://www.w3.org/TR/did-core/)

<sup>48</sup> [www.w3.org/TR/vc-data-model/](http://www.w3.org/TR/vc-data-model/)

<sup>49</sup> Preukschat, A., 2021. Self-Sovereign Identity.

type of credential), the holder shares the credential with the verifier who is able to check the validity of the credential against the Blockchain as well as the entity that has issued the credential.

*Figure 1515 - Self Sovereign Identity Framework*



*Source: Preukschat, A. (2021)*

#### **2.4.1 European Blockchain Service Infrastructure (EBSI) and European Self Sovereign Identity Framework (ESSIF)**

In 2018, a statement<sup>50</sup> establishing the European Blockchain Partnership<sup>51</sup> was signed by 27 EU Member States, Norway, and Liechtenstein (EBP). The EBP group is assisting the European Commission in establishing a European Blockchain Infrastructure (EBSI).

Mariya Gabriel, the European Commission's Commissioner for Digital Economy and Society, welcomed the declaration, saying, "Blockchain is a great opportunity for Europe and Member States to rethink their information systems, to promote user trust and the protection of personal data, to help create new business opportunities and to establish new areas of leadership, benefiting citizens, public services and companies."

The EBP declaration is intended to supplement the Tallinn Declaration on eGovernment. This political statement, signed in 2017 by Member States and EFTA nations, emphasizes the critical role of efficient and secure digital public services in realizing the Digital Single Market's full potential. The Tallinn Declaration commits European governments and EU institutions to provide digital public services at a level commensurate with the present pace of technological advancement in our society. As a result, government agencies must use digital technology to develop new capabilities or modernize current ones.

<sup>50</sup> <https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership>

<sup>51</sup> <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=381517902>

In February 2019, the European Commission announced the Connecting Europe Facility's (CEF) 2019 Telecommunications Work Programme, establishing the first financing conditions for EBSI. The Horizon 2020 programme-supported actions continued to offer options for contributing to the advancement of EBSI<sup>52</sup>.

EBSI is a collaborative effort of the European Commission and the European Bank for Reconstruction and Development. The objective is to use blockchain to speed the development of cross-border services for public administrations and their ecosystems in order to validate data and increase the trustworthiness of services. EBSI has been developing a network of dispersed nodes around Europe since 2020, enabling applications focused on certain use cases. EBSI is the first pan-European blockchain infrastructure, built on open standards and a transparent governance approach<sup>53</sup>. EBSI was founded on five fundamental concepts.

1. EBSI's management must be in the public interest, and it is accountable for restricting its use to public and commercial services that deliver a net public benefit to the population of the Member States collectively.
2. Governance: The EBSI governance framework will guarantee that decisions are made in accordance with stakeholder consensus.
3. Harmonisation: EBSI governance should promote and maintain technical requirement and architecture harmonisation in order to avoid the proliferation of protocols supported by or contradicting architectural assumptions.
4. Wherever practical, the codebase for all EBSI services and structures should be open source to facilitate auditing, security, and healthy competition among service providers, suppliers, and the private sector.
5. EBSI must not only comply with, but model compliance with, the GDPR's present interpretation and continuous refinement, in addition to complying with eIDAS and other legislation.

The EBSI platform is a network of peer-to-peer nodes. The European Commission runs EBSI nodes at the European level, while the EBP Policy Group obliged Member States' agencies operate EBSI nodes at the national level. Each node has the ability to generate and broadcast transactions that update the ledger.

EBSI promotes the development of cross-border services that assist residents and enterprises in managing their identification, educational credentials, and document registration.

Seven use cases are being investigated.

1. **Self-Sovereign Identity (ESSIF):** Enabling people to construct and govern their own identity across borders by implementing a Self-Sovereign Identity paradigm across Europe.

---

<sup>52</sup> [https://www.eublockchainforum.eu/sites/default/files/reports/EU%20Blockchain%20Ecosystem%20Report\\_final\\_0.pdf](https://www.eublockchainforum.eu/sites/default/files/reports/EU%20Blockchain%20Ecosystem%20Report_final_0.pdf)

<sup>53</sup> <https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/EBSI>

2. **Diploma Management:** Citizens get digital ownership over their educational credentials, considerably lowering verification costs and increasing public confidence in the legitimacy of papers.
3. **Document Traceability** is the process of maintaining immutable reference data for documents or other digital artifacts that can be used to prove their authenticity/integrity at a later stage and can be linked together to create a trustworthy, time-stamped audit trail.
4. **Trusted Data Sharing:** Ensure the secure exchange of data (such as IOSS VAT identity numbers and import one-stop shop) between EU customs and tax agencies.
5. **SME Financing:** Creating new sources of (co)finance for political activities in the areas of sustainable economy, innovation, and SME modernization via the establishment of an EU-wide debt financing platform.
6. **European Social Security Pass (ESSP):** Fraud and mistake are prevented by facilitating communication and data sharing between European nations and EU institutions.
7. **Management of Asylum Procedures:** Facilitation of the management of cross-border and cross-authority processes involving asylum seekers.

## 2.5 Results of the survey

This sub-chapter outlines the results of a survey done by EY on 100+ C-Levels from various business and institutions from both the public and private sector. The survey consisted in 20 open questions on their view of Blockchain technology as well as its applications in the sectors that were described in this chapter, namely Decentralised Finance, traceability and digital identity.

The survey<sup>54</sup> starts with asking participants to auto-evaluate their knowledge about emerging technologies, participants rated their knowledge on Blockchain 48 on a scale from 0 to 95, other technologies performed similarly with Artificial Intelligence with the highest score (53) and AR/VR with the lowest score (34). These results show how much room there is for growth for these technologies once the knowledge will reach higher levels, indeed the overall score is medium-lower and shows the necessity for executives to skill-up. The next question that respondent were asked was about the willing of adopt such technologies by companies, results showed that Blockchain is the second most desired technology to be adopted by companies (57/100), with Artificial Intelligence the only one scoring higher (74/100), this shows how the perceived impact on businesses is high for these technologies, indeed 89%<sup>55</sup> of respondents stated that is planning to invest in these technologies as well as in learning tools in order to have a better understanding of how they could be applied to their processes, only 4% plans to invest in the mere adoption without investing in the learning and only 7% stated that is not willing to invest in neither adoption nor learning.

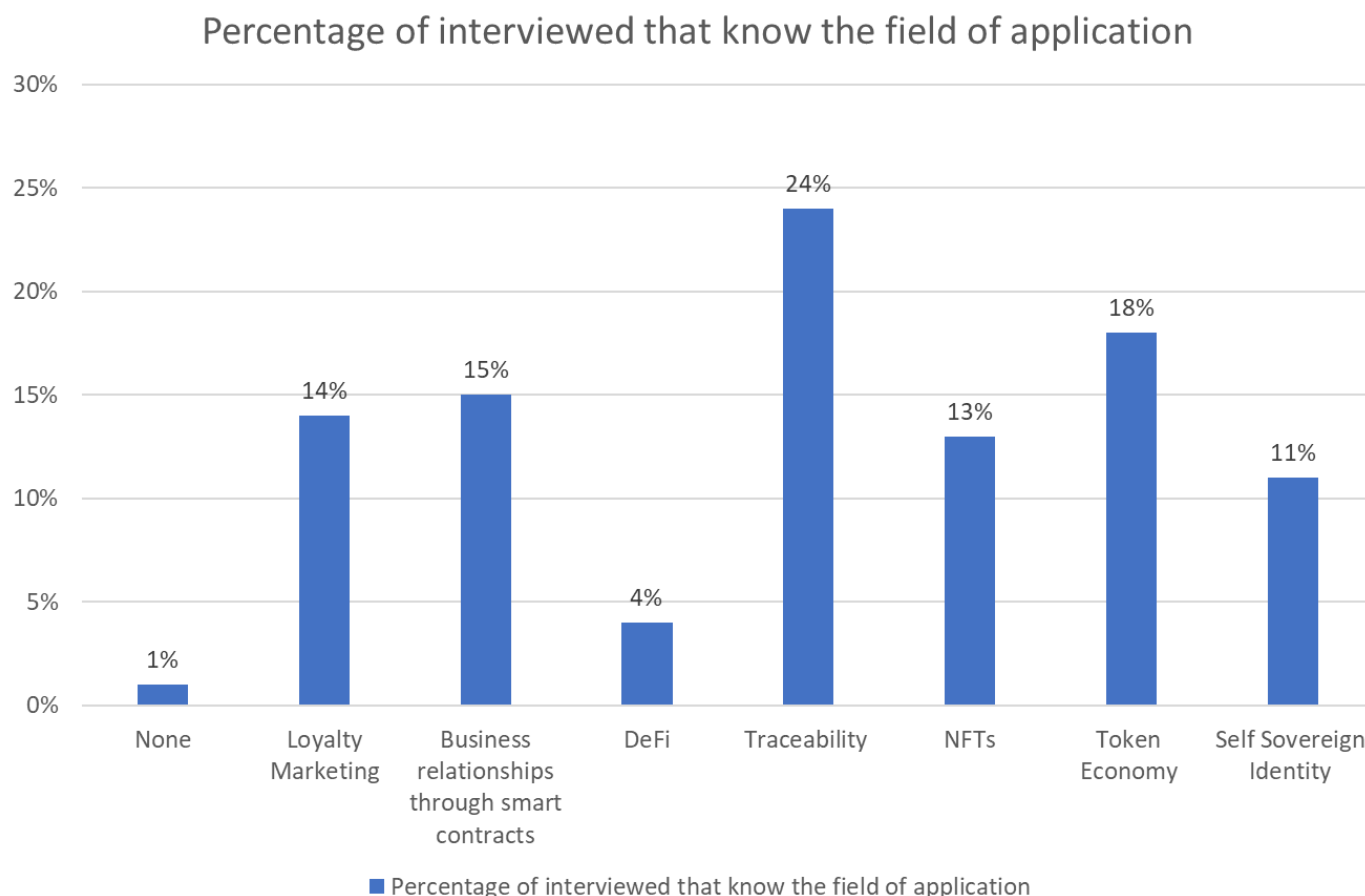
---

<sup>54</sup> [https://www.ey.com/it\\_it/news/2021-press-releases/11/ey-qiibee-blockchain-survey](https://www.ey.com/it_it/news/2021-press-releases/11/ey-qiibee-blockchain-survey)

<sup>55</sup> <https://www.qiibee.com/news/ey-blockchain-summit-survey-results/>

On average, C-Levels interviewed believes that such technologies will impact their portfolio of products by 41% in 3 years, 61% in 5 years and 80% in 10 years, these extremely high numbers show the awareness of the change that emerging technologies would bring to existing ecosystems.

Afterwards, executives were asked which were the field of application of Blockchain technology that they knew, the table below summarizes the results



Regarding traceability, one of the main fields of application for Blockchain, 58% of C-Levels interviewed believes that it is useful for both processes' optimization and marketing (intended as higher value of the products perceived by consumers), 29% believes that the technology only brings operational advantages derived from the tokenization of assets while 7% only believes in the communication power of Blockchain for consumers. Only 6% believes that the technology applied for traceability does not bring any value.

With regards to Self Sovereign Identity (SSI), participants were first asked about their willingness of adopting a system where identity is based on Blockchain and therefore data is in complete control of citizens/consumers, surprisingly 28% responded "absolutely yes", 31% said "probably yes", hence 59% of respondents looks positively towards the adoption of such a framework, the remaining part is divided as follows: 30% "maybe", 4% "probably not" and 7% "absolutely not". It is interesting how such a technology, that at a first glance would be seen as a technology with a moderate impact on businesses, being those private or public, benefits

from such high feedbacks by executives, but despite having to educate consumers / citizens on how to use this new technology, the latter can bring high values for businesses first of all can alleviate from the burden of external data protection. Indeed, having to comply with the existing regulations businesses need strict rules and standards for the storage of data coming from their users, hence if it can be avoided to even store it is a high-cost reduction opportunity for businesses. With regards to cost reduction self-sovereign identity brings other advantages, the major ones being:

- Efficiency in data exchange, thus reducing the need for manual verification and prove of data validity
- Identity verification costs
- Avoid data breaches

Finally, respondents were asked which were the main roadblocks towards the adoption of Self Sovereign Identity and these are the main problems they see toward the adoption:

- Lack of knowledge
- Compliance and legal issues
- Network Governance
- Lack of internal expertise
- Lack of clarity
- Privacy and Security
- Lack of interest in their own business

On the other hand, with regards to Decentralized Finance the path towards adoption seems to be very hard, if to ever happen. Indeed, 44% of respondents is not willing to use services offered by DeFi, such as staking, lending and borrowing, and slightly less than a third of the total respondents (26%) does not know the topic at all, the remaining part, 30%, is either using or will be using the services offered by Decentralised Finance. Among the main issues described by the executives: frauds, lack of contact with real consultants, lack of reliability and regulation are the main ones. It is totally understandable how such a topic is perceived negatively by respondents since it is something very new that brings with it a lot of news about frauds, hacking and anonymous people wanting to “bring down the traditional finance”, but it is also important to remember that DeFi basically born 1-2 years ago, therefore it still has a lot of time to be improved and to “rebrand itself”, naturally its destiny is strictly tied to that of cryptocurrencies adoption by institutional investors. Finally, the sample was asked what they thought about regulators and regulations concerning decentralised finance and

58% thinks regulators will include new rules to regulate the decentralised finance market, 39% think that any regulation will be restrictive for this innovative field and only 3% has no opinion on this.



# CHAPTER III - BLOCKCHAIN APPLIED TO THE SECURITIZATION

## 3.1. Introduction to securitization through blockchain

Token offers are gaining traction as a means of acquiring funds for businesses. Between 2017 and 2019, there were 2,064 digital asset offers (compared to 4,233 equity capital raisings through initial public offerings) totalling more than \$25 billion in financing<sup>56</sup>. According to some projections, digital securitizations of physical and financial assets would expand to roughly \$70 billion in financing by 2026, up from the current capitalization of about \$3 billion in 2020<sup>57</sup>. Access is currently reserved for businesses with a high volume of issuance, financial resources, and financial market expertise. Indeed, almost 60% of the world's resources are now unavailable through conventional market systems. Tokenization eliminates entry barriers, allowing any asset investable for a global investor base. We are discussing SME stocks, the real estate market, and a variety of "unbankable" assets that make for a significant portion of global wealth. Information asymmetry, limited investor access, and high transaction costs all contribute to the difficulty of accessing these markets.

Main issues are:

### **SME stocks:**

- Most SME stocks are unlisted
- Bond issuance is not provided
- Limited options beyond loans

### **Real Estate:**

- Local asset class
- High demand, but low liquidity
- Large tranches and large notes

### **Unbankable and illiquid assets (NPLs):**

- Accessible only to insiders
- No or limited transferability

---

<sup>56</sup> <https://thetokenizer.io/2021/03/23/azimut-launches-the-worlds-first-security-token-in-the-asset-management-sector-and-accelerates-on-the-synthetic-bank-project-in-the-digital-asset-economy/>

<sup>57</sup> [https://www.azimut-group.com/documents/20195/1674564/CS\\_AzimutToken\\_230321\\_ENG\\_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a](https://www.azimut-group.com/documents/20195/1674564/CS_AzimutToken_230321_ENG_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a)

Tokenization provides a number of advantages that fundamentally enhance asset holders' and investors' market access. Along with lowering total issuance costs, tokenization enhances asset accessibility and attractiveness:

- Low-cost issuance: Tokenization eliminates the need for an intermediary, therefore saving critical time and money.
- Fractional Ownership: At no extra expense, assets with large minimum ticket amounts may be fractionated.
- Transferability: With an all-digital infrastructure, asset ownership may be transferred instantly and globally.
- Rapid Execution: Time to market is reduced by standardizing and automating the issuance and management processes.

Leading organizations including as KPMG, Deloitte, and the World Economic Forum anticipate that 10% of global GDP will be tokenized by 2025-2027, creating a massive market opportunity for STO providers.<sup>58</sup>

### **3.2. Benchmark: existing blockchain based securitization platforms on the market**

In the following sub-chapters are described the main existing blockchain-based securitization platforms on the market as well as a description of the overall process adopted by them for the tokenization of credits or illiquid assets. Finally, in the last sub-chapter it is described a proposal on a technical level for the securitization using blockchain that builds upon existing solutions.

#### **3.2.1. Azimut**

Azimut Holding is a privately held corporation that is specialized in consultancy and asset management. Azimut provides a diverse selection of goods to meet a variety of market requirements, indeed, Azimut has launched the Azimut Token<sup>59</sup>, a cryptocurrency backed by a portfolio of 5 million euros in loans to small and medium-sized firms that were crowdfunded via the Borsa del Credito platform and are guaranteed by the Mediocredito Centrale Guarantee Fund. These loans are securitized and then "tokenized": anyone who purchases an Azimut Token<sup>60</sup> acquires a digital share of these loans and can trade it with other investors on a platform managed by Sygnum (Sygnum Bank), the world's first digital asset bank, authorized by the Swiss and Singaporean supervisory authorities. Thus, formerly "illiquid" assets such as loans to small and medium-

---

<sup>58</sup> "The future of asset servicing shaped by three disruptive technologies", Deloitte, 2017

<sup>59</sup> [https://www.azimut.it/documents/20195/1674564/CS\\_AzimutToken\\_230321\\_ENG\\_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a](https://www.azimut.it/documents/20195/1674564/CS_AzimutToken_230321_ENG_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a)

<sup>60</sup> <https://en.cryptonomist.ch/2021/07/22/azimut-luxembourg-gives-green-light-to-crypto-funds/#:~:text=Azimut%20and%20crypto%20Azimut%2C%20founded%20in%20Italy%20in,best%20market%20opportunities%20for%20every%20type%20of%20investor.>

sized businesses became universally accessible investments. The revolutionary scope of Azimut Token will also enable the company to accelerate the development of the Synthetic Bank project, through which Azimut wants to deliver 1.2 billion euros in loans to Italian SMEs between 2021 and 2025<sup>61</sup>: Businesses will be able to receive funding more promptly and at a lower cost. To date, Azimut's Synthetic Bank operations have benefited from the Group's fintech investments, particularly Azimut Capital Tech, in collaboration with Borsa del Credito, and Azimut Direct, in collaboration with Epic, which enable an efficient and rapid credit disbursement and risk management process.

### 3.2.2. Wizkey Define

WizKey is a company that provides innovative credit products and services to banks and financial institutions using a proprietary end-to-end platform based on cloud storage, artificial intelligence, and blockchain technology<sup>62</sup>. WizKey is the owner of a platform (Define) that allows financial operators to value their assets by converting them into secure, transparent, and liquid tokens<sup>63</sup>. WizKey allows its clients to quote credits on the global digital market thanks to the use of blockchain technology, making transactions faster and simpler and ensuring the automation of audit and due diligence processes. WizKey's solution disintermediates the credit market to generate value for financial operators while lowering transaction costs by learning about new global digital markets and recovering value through the elimination of competitive and costly activities. WiZKey has developed a decentralized platform based on blockchain technology for credit card transactions, structured finance transactions, and the distribution of financial products to banks, businesses, and financial intermediaries.

The Define Platform is a very adaptable tool, indeed WizKey's node architecture consists of a cloud component and a blockchain component (Ethereum), this combination allows to manage a large number of data points with speed, security, and ultimate confidentiality. WizKey is a third-party designer who, as a result, does not have access to any of the users' personal information. The data room<sup>64</sup> uses Artificial Intelligence capabilities to check for correspondence between credit documents and datatapes, alerting users to any discrepancies and reducing the risk of a claim. The flexibility of a data room's structure allows for the submission of one or several credit cards. The tokenization procedure entails notarizing a credit document on a public blockchain (Ethereum) in order to provide reliable facts and integrity to information. This results in a one-to-one and permanent connection between tokens and documents, with both being transferred at the time of cession. The

---

<sup>61</sup>

<https://www.azimutinvestments.com/documents/45685/52676/12.01.2021+FY+2020+Net+Profit+expected+between+375+and+415+million+euro.pdf/9e963b5a-f040-7f04-7179-69042c392a1e?t=1613667018084>

<sup>62</sup> <https://www.wizkey.io/it>

<sup>63</sup> <https://www.wizkey.io/it/wizkey-define>

<sup>64</sup> <https://www.wizkey.io/en/wizkey-define>

features of the blockchain and the architecture of the token allow the structuring of local and cross-border activities that are free of the hazards associated with informational anomalies in the acquisition of financial assets. These benefits translate into higher asset liquidity, increased ability to value for sellers, and lower risk for investors in the context of a possibly global crisis. The whole negotiating process is notarized to provide precontractual protection. The transfer of tokens on the blockchain, and therefore the transfer of credit ownership, is automated and safe owing to a delivery vs payment system that enables tokens to be distributed only when a successful payment has been made. Distinguishing features that the platform includes are:

- Smart Data Room: a virtual data room that is tied to a single credit for its whole lifecycle. The virtual data room provides limitless storage space and is portable: it is linked to each individual credit and can be transferred from one portfolio to another. Every credit, however, is permanently linked to its data room, preventing data loss during its lifecycle.<sup>65</sup>
- Increased granularity and maximized credit value over time
  - o Granularity: The platform enables users to create customized portfolios. Portfolio composition may be constructed in a number of ways and at a variety of granularities by using the data room's capabilities. The assignor may invite a large number of assignees, allowing them to cherry-pick certain names or participate on the building of a new portfolio, rearranging credits to match their demands.
- Selective collection of receivables
- Reorganizes receivables in accordance with the assignee's requirements.
- Agile Due Diligence: Simplifies and automates due diligence operations using AI. The due diligence procedure is expedited by an OCR that automatically compares the Data Tape to the underlying documents. The process's output is permanently associated with receivables, hence reducing information asymmetries and conflicts between data tape and paperwork.
- Tokenization: leveraging the blockchain's capabilities to maximize the value of structured finance transactions. Utilizing the Ethereum blockchain's capabilities, each credit is tokenized and thus represented by a standard token on the blockchain. Tokenization has the ability to convert traditionally illiquid assets, such as credits, into liquid, transferrable tokens. Therefore, the token itself becomes the asset, tokens are fungible and may be transferred instantly, finally, this allows further protection against the danger of fraud.
- End-to-end workflow: all stages of a structured finance transaction are programmed and may be completed inside Define, from transaction issuance to the settlement. Additionally, the use of notarization on the blockchain offers legal protection for the transaction's participants. Therefore, pre-contractual protection is guaranteed; transaction management is enhanced; and all processes are notarized on the blockchain.

---

<sup>65</sup> <https://www.wizkey.io/en/blog/privacy-wizkey-ensures-personal-data-protection-at-the-highest-level/>

WizKey has developed the ideal process for executing an endless number of receivables transfer and/or securitization actions on the platform. This process was developed to improve the service's value proposition to customers, namely by enabling deleveraging actions with little operational impact on internal resources, automating procedures, and increasing transaction transparency. WizKey exemplifies the following platform features:

It enables end-to-end credit lifecycle management as well as the creation of marketplaces for one's own financial assets (such as bonds and credits) and interaction with various categories of subjects (i.e. advisors, lawyers, investors, and servicers). It is configured to handle an infinite number of transactions. Moreover, the platform has been selected by SIA S.p.A. as a strategic partner for financial solutions utilizing blockchain technology for banks and financial intermediaries, and the strategic agreement between the two companies has already enabled them to acquire customers of primary standing, such as FCA Bank. Additionally, the platform, has been selected by Elite SIM S.p.A. as a partner for the development of financial solutions utilizing blockchain technology for banks and financial intermediaries, specifically, the platform will enable the achievement of two critical strategic goals:

1. Rationalization and automation of the credit deleveraging process, given that it enables the simultaneous execution of actions linked to the sale of credits and the issue of bonds, as well as the establishment of a main and secondary market for credits and financial products;
2. Increase the breadth of services supplied in accordance with the associated business plan: indeed, the platform's usage entails the establishment of a cloud/blockchain node that enables these clients to issue bonds and develop a secondary market for these financial instruments.

Advantages derived from the use of blockchain<sup>66</sup>:

- Generate significant operational savings through:
- Automation of processes: once the financial assets (in particular the receivables related to the transaction) have been tokenized it will be possible to manage them automatically through a set of smart contracts;
- Security and certainty in data sharing: one of the most widely recognized characteristics of blockchain technology is that, through the timestamping system incorporated in it, and since this system is neutral between the parties involved in the relative processes, the certainty regarding the information shared, the fact that it automatically has a certain date recognized for legal purposes and the non-corruptibility of the information substantially increase transparency. These benefit all the parties involved in the chain, generating important savings in terms of time and personnel, being able to rely on the data shared (e.g., in relation to the transaction, data regarding receivables)

---

<sup>66</sup> <https://www.wizkey.io/en/blog/tokenization-of-credits-%E2%80%93-token-erc-721/>

- Significant reduction of counterparty risks: the settlement on the blockchain network is instantaneous and it is possible to operate the so-called atomic swaps, i.e., for example, in the context of credit transfer operations, the ownership of the credit is passed on at the same time as the payment of the price through an automated smart contract system. The contextuality of the settlement thus significantly reduces counterparty risks;
- Compliance as-a-service and efficient management of collateral: the costs relating to compliance with regulatory regulations can be reduced to zero if the regulatory logic is implemented in the sets of smart contracts used by the platform. On the same platform, investors will be guaranteed, via a set of smart contracts, compliance with financial covenants regarding the quality of the receivables assigned and their ratio in relation to the debt assumed in this context;

Generate higher revenues due to:

- Increased liquidity of illiquid assets such as credits: the blockchain can incorporate the secondary market of any type of tokenized asset, thus starting from its characteristics, it is always possible for any buyer of tokenized assets to resell them to further investors being able to rely on the information already processed previously by third parties and thus being able to bring the due diligence activities already carried out to the benefit of the entire chain of financial assets (if tokenized);
- Simplification of processes: blockchain technology allows, for example, rapid bookbuilding for the issuance of bonds without having to be brokered by lead managers and/or arrangers;
- Possibility of fractioning investments: tokenized assets are infinitely divisible and this allows the enlargement of the investor base, in compliance with the applicable rules, to a much larger audience than the typical one of financial transactions since, from a technological point of view and thanks to bookbuilding and the dynamics of the secondary market described above, it is possible to propose a substantial fractioning of investments to reduce investors' risk;

### 3.2.3 Hypermasts

Hypermast STS positions itself as a tool for simplifying and standardizing securitization operations, with the ability to connect originator, servicer, intermediaries, credit institutions, and investors, allowing all securitization actors to interact in a transparent, safe, and traceable manner throughout the operation. Hypermast STS intends to simplify and transparent securitization operations in accordance with new European legislation.

The platform addresses essential procedures in securitization transactions, such as the development and signing of initial contracts (block sale), contracts underlying securities issue operations (block issue), and smart contract definition for the management.

Centotrenta Servicing SPA<sup>67</sup> created the platform in collaboration with IBM and Blockchain Reply, with BNP Paribas Securities Services serving as the custodian bank and paying agent.

The prototype was finished in November 2019 and addressed a number of key issues, including possible ways to interface with Bank of Italy systems (Infostat, FE129), security and user profiling issues, data protection management, and digital signature mechanisms that allow various actors to sign the HyperMast STS platform regulations and onboarding according to their role.

The prototype made use of a blockchain network made up of the key players involved in the sale and issue phases<sup>68</sup>:

- Arranger: node from which the origination of the transaction starts
- SPV: central organization of the securitization operation and main junction of the negotiation and contract signing activities
- Servicer: counterparty node of the SPV in which the negotiation activities of the contracts of the sale block are defined
- RON: node that defines the interfaces of the noteholders with the SPV for negotiation and signing operations
- Bank: represents the bank of the account / paying agent
- Calculation Agent: sub-node of the Servicer, interfaces with the SPV to define the contracts underlying the note payment relationships

The platform project has entered an industrialisation phase as of February 2020, and new network members, such as paying agents, originators, servicers, brokers, lenders and investors, law firms, and technological businesses, have been urged to participate.

### 3.2.4 Securitize

Founded in 2017, the San Francisco-based startup has raised about \$87.5 million in funding from an extensive list of investors including Coinbase, Sony, Morgan Stanley, Santander, Nomura, Sumitomo Mitsui Trust Bank, Blockchain Capital, and SPiCE VC<sup>69</sup>. Securitize produces net asset value (NAV) reports so anyone can see that the actual value of their tokens is based on the real assets they represent.

Securitize Markets is a member of FINRA<sup>70</sup>, is registered with the SEC and is a SIPC member.

---

<sup>67</sup> <https://bebeez.it/npl/centotrenta-servicing-lancia-hypermast-sts-piattaforma-standardizzare-cartolarizzazioni-crediti-basata-blockchain/>

<sup>68</sup> [https://centotrenta.com/wp-content/uploads/2020/02/Hypermast-CV-20191120-Press-Release\\_EN.pdf](https://centotrenta.com/wp-content/uploads/2020/02/Hypermast-CV-20191120-Press-Release_EN.pdf)

<sup>69</sup> <https://www.nanalyze.com/2021/09/securitize-complete-platform-securitization/>

<sup>70</sup> <https://www.finra.org/>

Securitize has created a platform that provides the tools for issuers to manage all elements of the digital securitization cycle, including Smart contracts that support token information on the Ethereum blockchain.

The Securitize platform allows users to manage their digital securities from a dashboard. The Digital Securities (DS) protocol ensures that digital securities issued through the Securitize platform can be traded in a compliant manner in all markets. The DS protocol<sup>71</sup> provides a compliant integration solution for issuers, investors and exchanges throughout the entire cycle, from initial issuance to trading, distribution and governance. The platform has the following features:

Is an end-to-end digital marketplace that brings issuers and investors together in a single platform, allowing users an easier experience in building and managing their portfolios. To start using the platform, users need to register, verify their identity and connect their bank account or wallet.

Exchangeability: the user has the ability to exchange selected holdings through the peer-to-peer trading platform.

Securitize offers end-to-end tokenization of funds, companies or assets. The securities are offered through Securitize Markets, LLC, a registered broker-dealer and FINRA/SIPC member. Through a partnership with 22x fund<sup>72</sup>, which represents equity in companies that participated in the 500 startups accelerator program in Summer/Fall of 2017, it has the ability to offer the securities tokens of 22 startups selected from the '500 startups Accelerator program'<sup>73</sup>, which includes the best startups in Silicon Valley. 22x fund is the idea of the founders of startups from the batch 22 of the 500 Start-ups Accelerator program to create a tokenized investment offering. The founders saw a great opportunity to raise capital together through an ICO. Through their partnership with Securitize Capital LLC, 22X Fund was born. The start-ups are represented by a token that seeks to give investors more liquidity and better returns.

Securitize AQUA: uses the same smart contract infrastructure as Securitize and is an alternative for issuers who want to provide investors with the benefits of tokenization, including the ability to transfer ownership quickly and compliantly without complicated paper-work processes. Investors holding securities in a portfolio on Securitize AQUA can access and manage their investments using the same Securitize dashboard used for securities running on public blockchains.

Securitize provides three types of offerings:

- Primary market: opportunities to fund start-ups, private companies and projects.

---

<sup>71</sup> <https://securitize.io/resources/protocols>

<sup>72</sup> <https://22xfund.com/>

<sup>73</sup> <https://500.co/>



- Secondary market: opportunities to trade digital asset securities in funding rounds with other investors.
- Securitize Capital Funds: actively managed digital asset fund providing exposure to cryptocurrencies that are uniquely enhanced by the return derived from proprietary lending activity.

### Securitize Strengths:

Institutional investors: Morgan Stanley's first blockchain investment was in Securitize. Japanese bank Sumitomo also used the platform to create Japan's first credit-rated security tokens, making Securitize the first blockchain company to receive significant institutional funding from North America, Europe and Asia-Pacific.

Full regulatory approval: the company has received full regulatory approval on all of their offerings, so they don't have to subcontract or rely on third-party processing. In 2020, they acquired a broker-dealer and alternative trading system, this decision was made after Securitize initiated communication with more than 40 firms who were planning to use the platform, with all the appropriate regulatory approvals, to trade securitized assets.

Size: Over the past four years, more than 300,000 verified investors have used the Securitize platform to support over 150 companies<sup>74</sup>.

### 3.2.5. Stonize

Stonize, founded in 2019, is a fintech start-up<sup>75</sup> offering a blockchain-based credit securitization platform recognized as the first BDLT fintech use case for the EU by the 'Use cases Working Group (WG6)' of the Technical Committee of the International Organization for Standardization on Blockchain and Distributed Ledger Technologies (ISO/TC 307)<sup>76</sup>.

Stonize is working with the Trust Theory and Technology (T3) group of the CNR's Institute of Cognitive Science and Technology (ISTC), the largest research institute in Italy, on a project involving the study of a framework to evaluate the trust of blockchain-based products and services.

It is an end-to-end platform through which the entire securitization process is managed:

1. Origination: i.e., managing the original asset, (such as invoices).
2. Onboarding: using digital and regulated KYC and AML processes, towards those who hold the assets.

<sup>74</sup> <https://securitize.io/press-releases/series-b>

<sup>75</sup> <https://stonize.com/>

<sup>76</sup> <https://standards.iteh.ai/catalog/tc/iso/06219ad2-2f1b-417b-ba56-3668066e8b99/iso-tc-307>

3. Tokenization: assets and securities are transformed into tokens, then providing information on their performance.
4. Transfer: With the transfer of ownership comes the issuance of securities, which are associated with a security token that is paired "one-to-one" with the original asset, represented by the basket of invoices. This token facilitates trading & settlement, enables the asset to be put into "circulation" and allows companies to exploit its value.
5. Notarization: Finally, notarization is used to provide accurate and rigorous real-time reporting of what is happening, enhancing the theme of transparency.

Stonize is not only a tokenization platform where a company accesses to obtain funding on the primary market, but also a model that accompanies the company providing guarantees on the performance in the life cycle of the asset and provides a workflow that allows to simplify the securitization operations by providing guarantees and data to attract funding.

Enablers: the blockchain used is the permissionless Algorand. The second key enabler of the solution is digital identity and the choice of eIDAS (electronic IDentification Authentication and Signature) compliance. eIDAS compliance helps to have certainty of the interlocutor because it is part of the characteristics of the digital trust services it introduced. The choice of Algorand is mainly driven by the fact that, being a PoS blockchain, the transaction in blockchain is implemented practically in real time: it provides a latency that varies from a few tenths of seconds to a maximum of 4.2 seconds in the case of complex transactions. Transactions do not run the risk of suffering DoS attacks and offers guarantees for the parties operating on the platform.

Main use case: The most "common" use case concerns invoice management. PA suppliers sell assets, invoices to an actor that issues security tokens, this actor can sell them to institutional investors, and with the proceeds pay back the suppliers. This actor becomes the owner of the credit and therefore is the creditor of the PA, collects the money as these invoices are paid and has a timely reporting activity and traceability of all operations.

Business model: marketplace model, it offers the platform as a tool, but also connecting services between originator and institutional investor. The start-up is multistakeholder, it has relationships with financial service providers that operate securitization, including custody service providers. Stonize aims to increase interoperability through a platform that allows network players to interact in a secure and reliable way, providing data to investors to enable investment choices and giving the originator the possibility to raise funding quickly and at competitive costs.

### 3.3. AS-IS: Securitization of credits using the Blockchain

The securitization process involves two flows:

Sales flow: the asset is placed on the market in the form of a token with a rating provided by the platform used. This flow foresees the possibility for sellers to update the information available regarding the positions offered.

1. Purchase flow: the user/entity, after being identified and approved by the platform, purchases the asset in the form of a token and has the possibility of monitoring it over time (also post-purchase) via the platform.
2. Creation: during the creation phase, the seller decides whether to list a portfolio of assets or a single asset, entering the necessary data in a document containing the relevant information of the position.
3. Rating: the platform performs an initial check to assess the completeness of the data quality and assigns a rating. The seller has access to the simulation area of the pricing tool where he can calculate the value of his assets using parametric mathematical models.
4. Tokenization: once the seller is satisfied with the data quality, the tokenization process begins and the creation of representative security tokens directly on the platform.

Selling: sellers have the ability to send accredited investors to the platform, manage all data (KYC / AML), allowing investors to operate and trade on the platform. Position information can be updated and transactions can be approved via transfer agent functions also on the secondary market.

In order to ensure compliance during issuance/transfer, the figure of the on-chain, the Transfer Agent is envisaged, i.e., a centralised authority managed by the issuer able to control all transactions. In particular, the Transfer agent can carry out:

- Digital onboarding and token assignment
- Transfer of authority to another centralized figure (e.g.: notary)
- Total control of the securities offering (mint-burn tokens etc.)

When Security tokens are issued, they are only assigned to eligible and approved investors.

Finally, vendors are able to execute: KYC online process, on-chain investor whitelisting (only approved addresses can transact on the blockchain), direct communication with the approved investor.

Secondly the purchase flow is described below:

1. Access: after being invited by the issuers, the potential buyer performs the KYC directly through the platform, so that they can analyse the data uploaded to the platform and view the general information of the positions

2. Approval: only after being approved, the investor is whitelisted, the blockchain address is then verified and the user/entity can check all the PDF documents associated with the positions and perform their own evaluations.
3. Purchase: after choosing the investment, the investor executes the bank transfer and receives the security token, which incorporates all relevant information and effectively represents the investment made
4. Monitoring: the investor can monitor the lifecycle of the position, updated by the seller. Moreover, he has the possibility to approve all transactions, through the transfer agent functions, even on the secondary market.

#### **3.4.1. Smart contract services**

When the tokenization occurs, all underwriting information relevant to the securitization transaction (e.g., representations and warranties, rating/scoring, borrower financial status, balance sheet information) is entered into a Smart Contract. This enables compliance with current regulatory and European Central Bank (ECB) requirements on loan-level data. The token also allows for exceeding these minimum requirements, as it is capable of including entire loan files, including collateral agreements, documents attached to collateral, appraisals, etc. However, the depth of available loan information also depends on the blockchain used and the design of the Smart Contract.

Figure 16 - Creation of the token by the seller

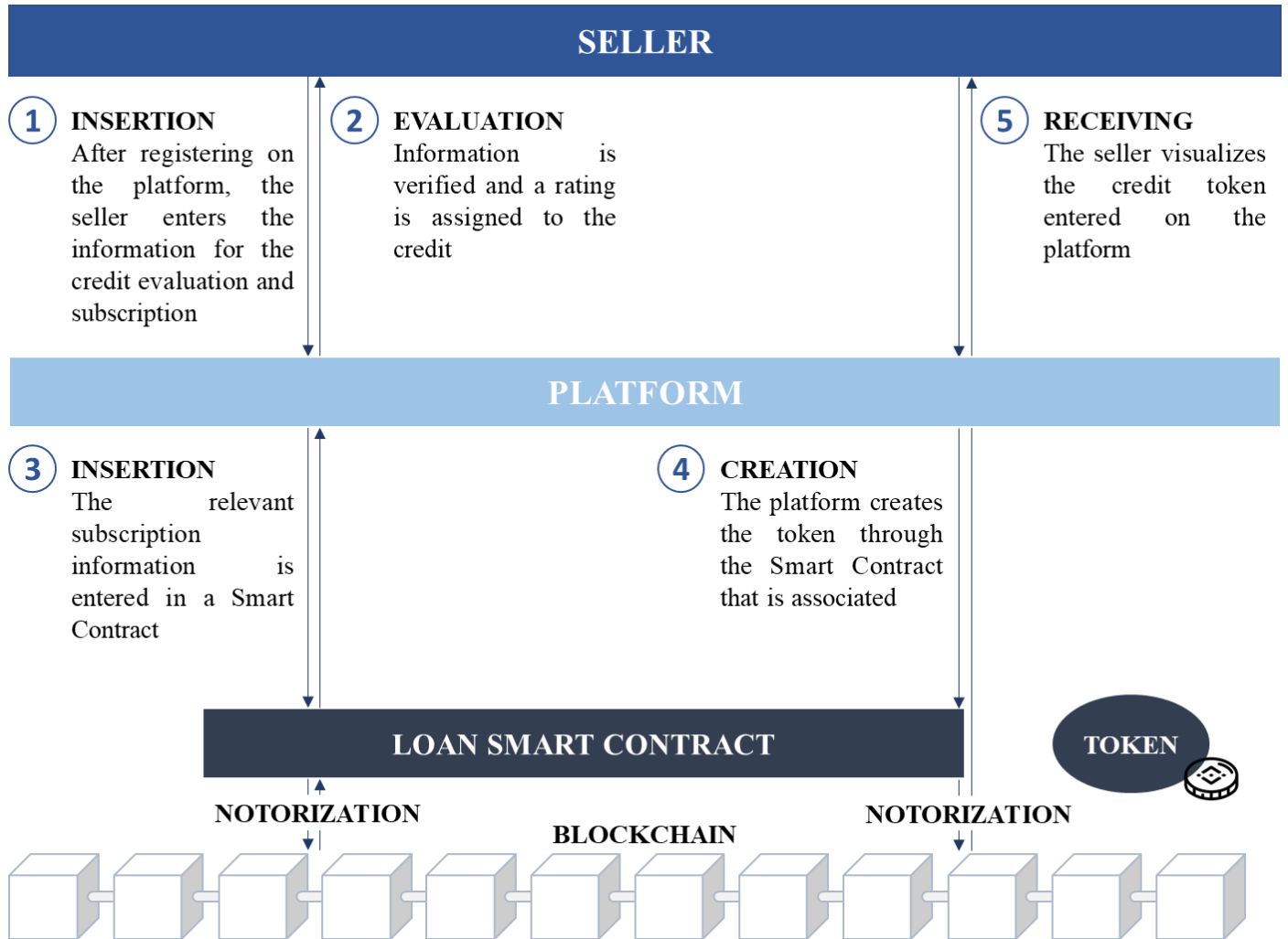
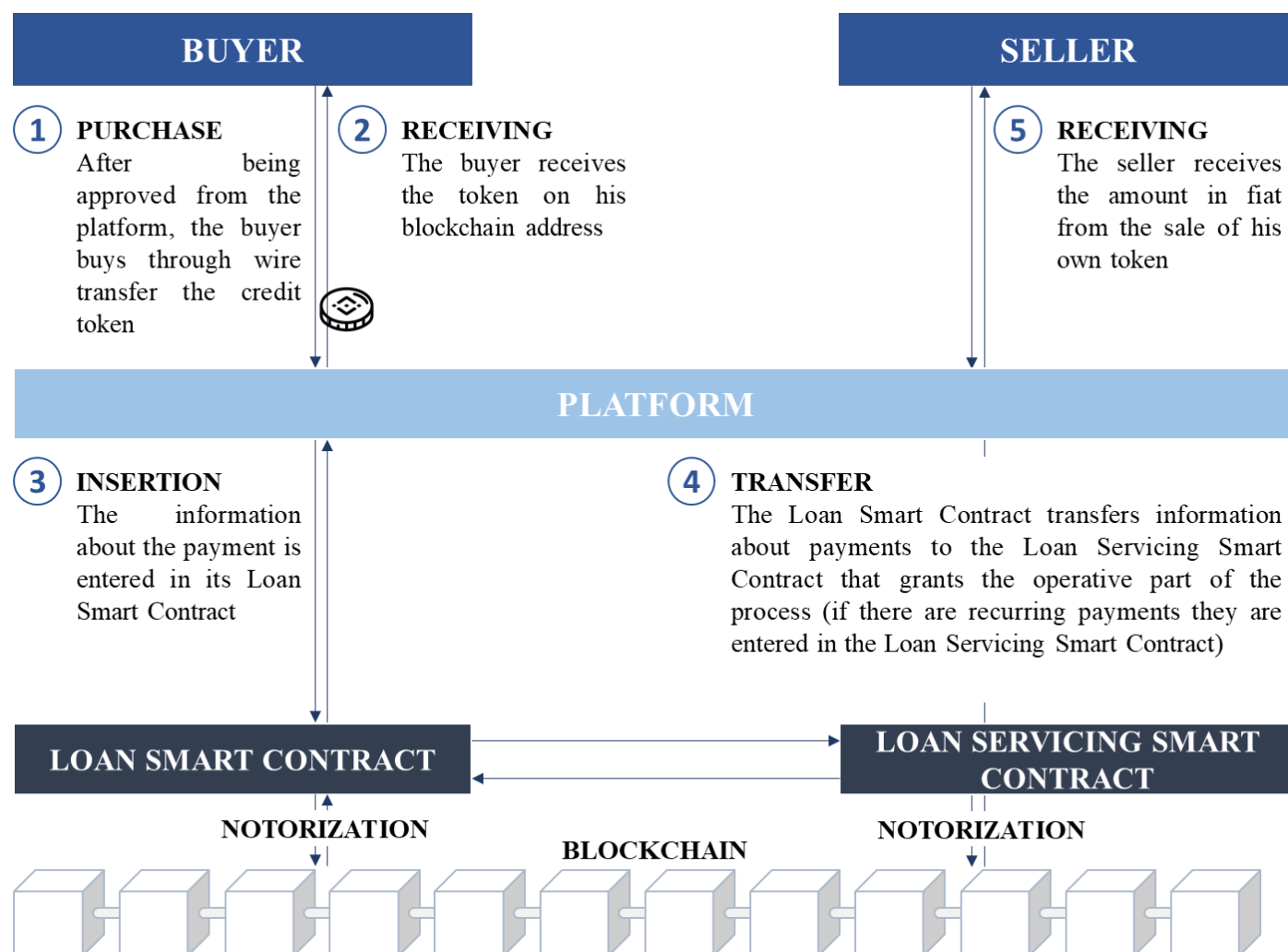


Figure 17 - Purchase of the token by the buyer



Contracts and tokens can be continuously updated and modified, reflecting information related to borrower payment behaviour, loan modifications, ongoing correspondence between lender and borrower, as well as other credit-related information.

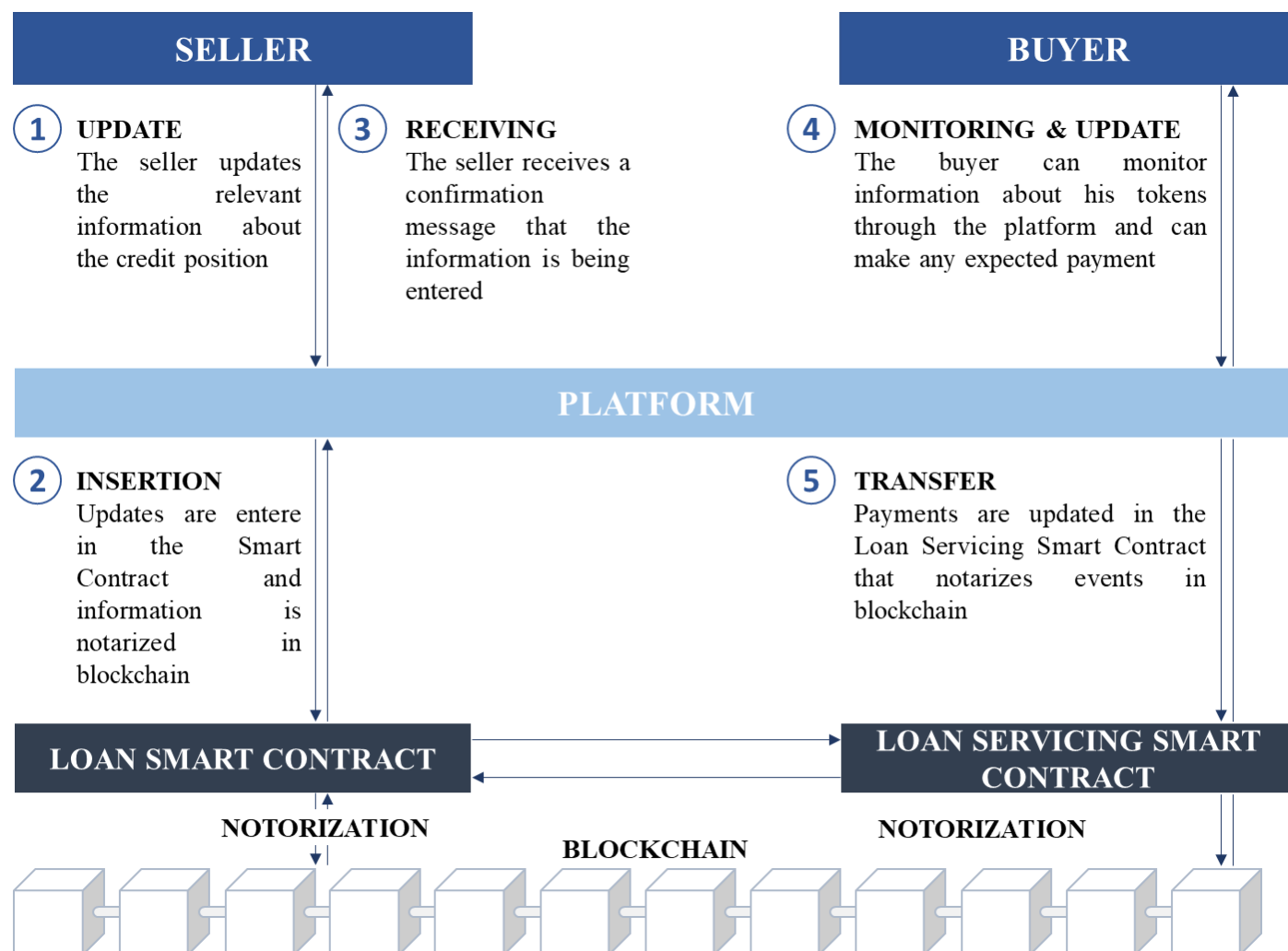
The compliance of loan-level characteristics with the eligibility criteria for a securitization transaction can be checked automatically, without using an external auditor. This is accomplished through a matching routine between the individual loan and a smart contract for the securitization transaction, which checks for portfolio eligibility criteria and/or guidelines. Each individual loan with a profile that matches the transaction's eligibility criteria is marked as "eligible" and added to the transaction's portfolio. Loan information available from smart contracts and tokens is used to update portfolio characteristics on a recurring basis.

All relevant information required for loan servicing is transmitted from a loan smart contract to a loan servicing smart contract. The loan servicing smart contract verifies and sends payments collected on performing loans into the blockchain in the form of tokens.

Smart contracts can be used to track new business by tagging each loan transferred to buyers. Labelling loans in the blockchain prevents from fraudulent double attribution of assets to more than one creditor.

Only one token per asset/loan can exist in an originator's entire loan record, and that token can contain a flag to indicate a previous lien.

*Figure 18 - Update of information and additional payments*



**Insolvency management:** when a borrower misses a payment and a loan becomes insolvent, the servicing smart contract automatically sends a reminder to the borrower. If the insolvency persists, the smart contract can automatically transfer the loan to a special third-party servicer with access to the blockchain. The loan file and asset token would be updated accordingly.

If a loan defaults, all relevant information about the workout, as well as related recovery proceeds would be placed on the blockchain. Payments would be directed between smart contracts through the tokens as previously outlined.

# CONCLUSION

The purpose of this work, as stated at the outset, was to investigate the unique and diverse prospects presented by Blockchain, particularly in the financial sector, but not only: asset traceability and digital identity have been found to be two use cases where blockchain is able to bring considerable value. We may conclude that Blockchain technology is well-suited for deployment in the business sector, which, due to its diversity and unique vertical requirements, requires a flexible, interoperable, transparent, automated, and tamperproof technology. Therefore, not only the Blockchain will have a big influence on the financial sector, but it will also be a cross-industry revolution.

In one year working on driving adoption of Blockchain technology by both the private and public sector I had the opportunity to partake on several meetings with professionals, top management and connect with the highest experts in this sector, hence I would highlight some elements:

- Top management, regardless of the sector, is well aware of the potential of this technology and is laying down resources to study and experimenting with it.
- Self-Sovereign Identity (SSI) is one of the most underrated use cases where Blockchain has an extremely high potential. Although the public sector is heavily exploring with it (e.g European Self Sovereign Identity Framework) the public is still unaware of it and of the already discovered potential it can bring into our day-to-day life.
- Blockchain, by enabling cross-platforms ownership of digital assets will bring completely new business models
- Blockchain adoption is seen as something complex and unaffordable even though it is not, since most of the times solutions require just the addition of an infrastructural layer over existing systems.
- Many times, the willingness to explore with this technology leads to a “find the problem for this solution” approach instead of “find the solution for this problem”.

Lastly, I would conclude with a focus on the last use case described, or, tokenisation of illiquid assets. Asset tokenization, enabled by blockchain technology, has long been touted as a mechanism for investors to get access to and alter their assets. While the promise of liquidity, automation, and transparency are all significant enhancements over the present system, true financial engineering has been largely ignored until now. The bulk of tokenized assets are pre-existing private and illiquid assets and securities that have been converted into tokens that reflect the original asset's worth and whose values change in response to supply and demand. It was widely anticipated that if enough issuers produced digitally represented private securities, market participants would spontaneously establish huge pools of secondary liquidity for these illiquid assets.



Nonetheless, without market makers, it has not transpired, and the predicted liquidity has not materialized. Indeed, although Blockchain technology may be the answer to trust and facilitator of peer-to-peer marketplaces, it is insufficient on its own to allow such markets to emerge and thrive. While blockchain enables new possibilities, it is only a technology that may serve and provide significant value when combined with other levers. Cost savings, fractional ownership, higher liquidity, faster settlement, immutable ownership records, and automatic compliance are all benefits of tokenization. All of these benefits are significant, but they do not always result in the production of new financial products or an increase in demand. They may expand the addressable audience by permitting the trading of formerly illiquid assets, but this does not always result in the creation of new demand. Notably, although a new class of investors has access to new asset classes, there is no forward connection to maintain a sequence of activities beyond asset formation and acquisition; rather, it is the prospect of infinite future transactions that produces demand and long-term value. To thrive in financial innovation, digitizing platform companies must have a full understanding and knowledge of securities regulations, as well as a collaborative approach to resolving regulators' concerns. Only a few fintech enterprises specializing in digital securities have an in-depth understanding of the regulatory environment, asset knowledge, and complementary skill sets throughout the investor ecosystem. These are excellent examples of how combining financial engineering with blockchain technology may result in the formation of a new class of investable asset or a major boost in the liquidity of underlying securities. While they are presently fairly small structured finance transactions centered mostly on retail, they represent promising initial steps.

## BIBLIOGRAPHY

- A. M. Antonopoulos, “Mastering Bitcoin 2nd Edition” - Programming the Open Blockchain, 2018
- M. Swan, “Blockchain: Blueprint for a New Economy”, 2015
- Coin Gecko, “How to DeFi – Beginner”, 2021
- Coin Gecko, “How to DeFi – Advanced”, 2021
- A. M. Antonopoulos, “Mastering Ethereum: building smart contracts and dapps”, 2018
- G. Comandini, “Da zero alla luna”, 2020
- N. Szabo, "The Bitgold proposal", 2005.
- M. Swan, “Blockchain: blueprint for a new economy”, 2015.
- V. Buterin, “A next-generation smart contract and decentralized application platform Ethereum”
- A. Back, "Hashcash - a denial of service counter- measure", 2002.
- D. Tapscott, “Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World”, 2018
- EY Report, “Applying IFRS, Accounting by holders of crypto-assets”, 2018
- Haber, S., Stornetta, W.S. How to time-stamp a digital document. J. Cryptology 3, 99–111 (1991)
- D. Chaum, "Untraceable Electronic Cash", Goldwasser S. (eds) Advances in Cryptology — CRYPTO’ 4 88, 1990.
- R.C. Merkle, "Protocols for public key ecosystem”

# SITOGRAPHY

<https://www.statista.com/statistics/1237821/defi-market-size-value-crypto-locked-usd/>

[https://www.azimut-group.com/documents/20195/1674564/CS\\_AzimutToken\\_230321\\_ENG\\_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a](https://www.azimut-group.com/documents/20195/1674564/CS_AzimutToken_230321_ENG_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a)

<https://en.bitcoinwiki.org/wiki/SHA-256>

<https://andersbrownworth.com/blockchain/>

[https://en.bitcoinwiki.org/wiki/Merkle\\_tree](https://en.bitcoinwiki.org/wiki/Merkle_tree)

<https://github.com/tendermint/tendermint/wiki/Block-Structure>

<https://consensys.net/blog/metamask/>

<https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys>

<https://www.fintechna.com/articles/nfts-and-the-cryptoverse/>

<https://opensea.io/>

<https://dune.xyz/rchen8/opensea>

<https://coinmarketcap.com/exchanges/blockchain-com-exchange/>

<https://bit-news.ch/2021/07/ethereum-heads-to-100k-tps-buterin-talks-about-post-merger-future/>

<https://ethereum.org/en/>

<http://ethdocs.org/en/latest/introduction/what-is-ethereum.html>

<https://ripple.com/ripplenet/>

<https://ripple.com/xrp/>

<https://www.fool.com/investing/2018/02/01/3-cryptocurrencies-processing-1500-or-more-transac.aspx>

<https://xrpl.org/>

<https://soliditylang.org/>

<https://coinmarketcap.com/alexandria/glossary/total-value-locked-tvl>

<https://defillama.com/>

<https://defillama.com/chains>

<https://defillama.com/chains>

<https://blockfi.com/>

<https://aave.com/>

<https://compound.finance/>

<https://medium.com/@gettyh/compound-finance-asset-risk-e4025487fcbb>

<https://uniswap.org/>

<https://finematics.com/impermanent-loss-explained/>

<https://www.undp.org/publications/blockchain-agri-food-traceability>

[https://www.ey.com/en\\_gl/news/2019/11/ey-blockchain-platform-supports-blockchain-wine-pte-ltd-to-launch-tattoo-wine-marketplace-across-asia-pacific](https://www.ey.com/en_gl/news/2019/11/ey-blockchain-platform-supports-blockchain-wine-pte-ltd-to-launch-tattoo-wine-marketplace-across-asia-pacific)

<https://www.digitalvoice.it/blockchain-tattoo-wine-prima-piattaforma-e-commerce-del-vino-per-il-mercato-cinese/>

<https://coinidol.com/carrefour-italy-tracks-food-using-blockchain/>

[https://www.ansa.it/sito/static/ansa\\_check.html](https://www.ansa.it/sito/static/ansa_check.html)

[www.w3.org/TR/did-core/](http://www.w3.org/TR/did-core/)

[www.w3.org/TR/vc-data-model/](http://www.w3.org/TR/vc-data-model/)

<https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership>

<https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=381517902>

[https://www.eublockchainforum.eu/sites/default/files/reports/EU%20Blockchain%20Ecosystem%20Report\\_final\\_0.pdf](https://www.eublockchainforum.eu/sites/default/files/reports/EU%20Blockchain%20Ecosystem%20Report_final_0.pdf)

<https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/EBSI>

[https://www.ey.com/it\\_it/news/2021-press-releases/11/ey-qiibee-blockchain-survey](https://www.ey.com/it_it/news/2021-press-releases/11/ey-qiibee-blockchain-survey)

<https://www.qiibee.com/news/ey-blockchain-summit-survey-results/>

<https://thetokenizer.io/2021/03/23/azimut-launches-the-worlds-first-security-token-in-the-asset-management-sector-and-accelerates-on-the-synthetic-bank-project-in-the-digital-asset-economy/>

[https://www.azimut-group.com/documents/20195/1674564/CS\\_AzimutToken\\_230321\\_ENG\\_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a](https://www.azimut-group.com/documents/20195/1674564/CS_AzimutToken_230321_ENG_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a)

[https://www.azimut.it/documents/20195/1674564/CS\\_AzimutToken\\_230321\\_ENG\\_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a](https://www.azimut.it/documents/20195/1674564/CS_AzimutToken_230321_ENG_FINAL.pdf/8268a62f-2d09-410a-ac56-5e2f065e136a)

<https://en.cryptonomist.ch/2021/07/22/azimut-luxembourg-gives-green-light-to-crypto-funds/#:~:text=Azimut%20and%20crypto%20Azimut%2C%20founded%20in%20Italy%20in,best%20market%20opportunities%20for%20every%20type%20of%20investor>

<https://www.azimutinvestments.com/documents/45685/52676/12.01.2021+FY+2020+Net+Profit+expected+between+375+and+415+million+euro.pdf/9e963b5a-f040-7f04-7179-69042c392a1e?t=1613667018084>

<https://www.wizkey.io/it>

<https://www.wizkey.io/it/wizkey-define>

<https://www.wizkey.io/en/blog/privacy-wizkey-ensures-personal-data-protection-at-the-highest-level/>

<https://www.wizkey.io/en/blog/tokenization-of-credits-%E2%80%93-token-erc-721/>

<https://bebeez.it/npl/centrotrenta-servicing-lancia-hypermast-sts-piattaforma-standardizzare-cartolarizzazioni-crediti-basata-blockchain/>

[https://centotrenta.com/wp-content/uploads/2020/02/Hypermast-CV-20191120-Press-Release\\_EN.pdf](https://centotrenta.com/wp-content/uploads/2020/02/Hypermast-CV-20191120-Press-Release_EN.pdf)

<https://www.nanalyze.com/2021/09/securitize-complete-platform-securitization/>

<https://www.finra.org/>

<https://securitize.io/resources/protocols>

<https://22xfund.com/>

<https://500.co/>

<https://securitize.io/press-releases/series-b>

<https://stonize.com/>

<https://standards.iteh.ai/catalog/tc/iso/06219ad2-2f1b-417b-ba56-3668066e8b99/iso-tc-307>