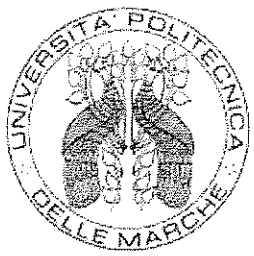



UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea Magistrale o Specialistica in International Economics and Commerce

# The usage of the blockchain technology in financial frauds:
# The Fyre Festival Case

Relatore: Chiar.mo
Prof. Samperna Simone

Tesi di Laurea di:
Suzeneide Luquene Cardoso de Sousa

Anno Accademico 2018 – 2019

**THE USAGE OF THE BLOCKCHAIN TECHNOLOGY IN THE PREVENTION OF FINANCIAL FRAUDS: THE FYRE FESTIVAL CASE**

# Summary

## Abstract

Viviamo in mondo dove la tecnologia è diventata parte integrante delle nostre vite, rendendo molte operazioni che in passato potevano risultare complesse, semplici ed effettuabili direttamente dal nostro divano. La facilità con cui con cui abbiamo accesso alla tecnologia, richiede però come sacrificio la condivisione dei nostri dati personali, rendendoli vulnerabili ed esposti a rischi di ogni genere, non sono come individui ma anche come imprese. Lo scopo di questo elaborato è quello di analizzare l'avvento della "nuova internet" rappresentata dalla tecnologia blockchain che con il suo libro mastro e sistema distributed, nata originariamente per trattare le transazioni della criptovaluta blockchain, possono essere adoperate anche in altri ambiti come le transazioni finanziarie o la prevenzione alle frodi, che è il tema principale di questa tesi. Nel primo capitolo verrà fatta un analisi di ciò che rappresenta la blockchain, dalla sua storia, ai suoi sistemi di funzionamento. Mentre nel secondo capitolo verrà spiegato come l'utilizzo della

tecnologia blockchain può essere adoperato a livello di corporate governance in ogni suo aspetto. Nel terzo capitolo invece verrà affrontato il tema introduttore del nostro caso studio, la frode. Verrà data una overview della storia della frode, quello che significa ed i casi più significativi della storia così come l'evoluzione del fenomeno.

Nel ultimo capitolo verrà spiegato il caso di frode finanziaria preso in analisi che è il Fyre Festival case, dal suo ideatore alle conseguenze penali che ha ottenuto, ed infine verranno fatte delle considerazioni su come l'utilizzo della blockchain può essere utilizzata nel ambito delle frodi, non soltanto nella risoluzione degli stessi, ma anche e soprattutto nella prevenzione.

## Introduction

Technology has become an integral part of our lives, making many operations that in the past could be complex, simple and can be carried out directly from our sofa. The ease with which we have access to technology, however, requires as a sacrifice the sharing of our personal data, making them vulnerable and exposed to risks of all kinds, they are not as individuals but also as businesses. The purpose of this elaborate is to analyse the advent of the "new internet" represented by

blockchain technology which with its ledger and distributed system, originally created to deal with blockchain cryptocurrency transactions, can also be used in other areas such as financial transactions or fraud prevention, which is the main theme of this thesis. In the first chapter an analysis will be made of what the blockchain represents, from its history, to its operating systems. While in the second chapter it will be explained how the use of blockchain technology can be used at corporate governance level in all its aspects. In the third chapter, however, the introductory theme of our case study, fraud will be addressed. An overview of the history of fraud will be given, what it means and the most significant cases of history as well as the evolution of the phenomenon.

The final chapter will explain the case of financial fraud taken into analysis which is the Fyre Festival case, from its creator to the criminal consequences that it has obtained, and finally considerations will be made on how the use of the blockchain can be used in the field of fraud. , not only in their resolution, but also and above all in prevention.

# I CHAPTER

## 1. The Blockchain

## 1.1 Blockchain General Identification

The technical definition of blockchain is "decentralized ledger and cryptographically secure transactions. " More generally, it is a technology that allows you to exchange not only information on the internet but, for the first time, also property. So not just the payment or exchange of goods and services, but, thanks to this innovation, any other form of collaboration between men will be able to take advantage of the possibilities offered by the network. Also “The Economist [1]"tried to provide a simplified explanation: *blockchain can be viewed as a sequential spreadsheet of operations, constantly update on a global computer network, which serves as a ledger distributed.* So when we talk about blockchain, we are referring to a registry safe international, shared by all those who act within one specific computer network, based on peer-to-peer technology[2]. The chain has the peculiarity of recording and archiving all the transactions that are carried out within that network, not making the presence of third parties necessary, so-called trusts. The blockchain name originates from the nature of the structure: each node in the network has a specific function in the assessment of the information

[1] Consulted on 04.11.2019: https://www.economist.com/leaders/2015/10/31/the-trust-machine
[2] Consulted on 08.11.2019: https://bitcoin.org/bitcoin.pdf

entered, which is transmitted to the next node in one block chain, the blockchain. Until a couple of years ago the block sequence was used only by Bitcoins as a kind of account book. All transactions carried out to date and verified are recorded in it directly from the system. The transactions, in fact, are feasible only if they receive approval by 50% + 1 of the nodes. The attention paid to the blockchain by the financial giants institutional, allows to hypothesize that it will become the operational philosophy of the banking and financial system of the future. This hypothesis becomes very close to reality if one analyses the trends of the use of architecture as much as technological innovation applied to it. The European Banking Association[3] has, in one of its reports, expressed a positive opinion about the system's reliability. The main feature of the whole architecture computer science can be summarized with a single term: decentralization. In fact, there is no central repository in the blockchain but a peer-to-peer between users, by entering transactions in blocks. In a blockchain architecture, transactions are created by the active components inserted in the network: the active user is defined as node and transfers Bitcoin to another node inserted in the network. The network blocks are created, in chain, by other subjects participating in the architecture that are defined miners. To create blocks, miners have to solve

[3] European Parliament Pdf consulted on 10.10.2019: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_IT.pdf

complex algorithms and, if they succeed, they are rewarded with Bitcoins. Since the user who manages to create a block gets 25 Bitcoins as a reward, inside of the aforementioned block, the "generation transaction" is recorded, ie that the transaction that allowed to create the block is always placed at first place within it, which will then be followed by other transactions validated[4]. The newly created transaction is distributed and validated following a rigid verification protocol to avoid, among others, the problem of "double spending problem ". In practice, the validity of a transaction is confirmed with the consent of the network nodes according to parameters set for the operation of the network itself; the knots that they validate are rewarded with Bitcoins. Just checked the validity of the transaction, the miners put it in a block and the transaction is executed with full respect for privacy. Very relevant is the characteristic of making the data immutable forever, reliable, searchable by everyone. Applying this technology could manage, for example, transactions related to the exchange of goods and services, the management of information related to Smart Contracts and disciplines and process procedures, payments.

### 1.2 History

Blockchain is the most advanced alternative to the centralized ledger, where management logic corresponds to the One-To-Many model. In this old type of

[4] Tim Mathis,2016 Ebook: A Guideline to Blockchain, the technology behind bitcoin

organization, everything is managed by the central authority. In fact, this is precisely how the organizational structure of the communities has always been conceived, where all the paper registers were centralized and under the control of the central authority.

Year Zero

In communities, organized into hierarchical and centralized structures where power was recognized only in the top authority, the need to create a register to annotate and maintain property memory was born, births, taxes, etc. This led to the birth of the ledger managed with the same organizational logic as the community; That is, the central authority dictated the rules for compiling and managing the registry and held ownership and power. The organization of public archives and also of other large private organizations, which had a great weight on society, for example banks, has never been questioned for many centuries. The first digital evolution even digitalization, for many years since its inception, has failed to change the organization of archives that have maintained the logic of centrality. Computerization has made archive management more agile, but nothing has changed in organizational logic since the paper age. This is also evident from the value attributed to the need to sign documents manually and how many procedures were required to have the documents in the original. The Public Administration and the large private financial institutions have continued to

manage the centralized system and the Central Ledger based on their authority. In this type of organization, therefore, the Public Administration and banks, as central authorities, are the only ones to have the power to update, make public and if necessary certify the contents of the ledger. Anyone who wants to access, for example, a mortgage must prove that they have a balance sheet that allows them to pay off it and this, even today, is only possible by obtaining certification of the ownership of real estate from the PA's Catasto and financial stabilities from the reference bank[5]. The central authority's position of strength that can determine the arbitrariness of the rules that make up the Central Ledger Governance is the limit of the centralized system.

The variant of the Central Ledger:

The Decentralized Ledger is the first variant to the Central Ledger, but the differences do not produce interesting effects. The central authority, in fact, with the Decentralized Ledger reproduces the centralized logic through peripheral principals called satellites, of which it maintains full control. In detail, the central authority operates with the organizational scheme of One-to- many against satellites, while the satellites operate with the model of One-to-many towards users.

[5] Imrar Bashir, 2018: Mastering Blockchain

## The real change: THE BLOCKCHAIN

The digital archive that represents the real innovation compared to the Central Ledger is Distributed Ledger. It is a database based on logic distributed over a peer-to-peer network that sees the archive played in full and faithfully across all nodes in the network, with the elimination of the central authority. Deleting the central authority results in the lack of control over the information placed in the archive. The main feature of the Distributed Ledger is the inability to lose data because the database is present on all nodes and software updates and avoids the user overwriting existing data; The system, however, does not have the ability to verify the quality and correctness of the information entered in the database. Further advancement in digital technology also allows the concept of Distributed Ledger to evolve, introducing control over the information that is intended to be included in the database, creating a new system called Distributed Ledger Technology (DLT). The task of the control, attributed in the Central Ledger to the central authority, in DLT is replaced by the achievement of the consensus that represents the success of the control, performed freely by one of the nodes, accepted and shared by the other network nodes. Auditing is done by applying a set of rules, shared by all network participants, that make up the governance of the system. A further evolution of Distributed Ledger Technology is the way in which consensus is achieved. The criterion remains the same, but the way in which the

information entered in the archive is made immutable and secure is to use codes and package the information in blocks, determining the birth of the blockchain.

### 1.3 The Blockchain's Ledger

The Blockchain's Ledger[6] is a decentralized archive on a user-to-user (peer-to-peer) network and, due to its characteristics, is the most advanced available today. The Blockchain Master Book is an evolution of Distributed Ledger Technology (DLT) from which it differs in the way of reaching consensus. The consensus criterion, on the other hand, is the same, and for the way to make the information stored with the use of codes and a structure called block is immutable. The block, upon reaching consensus, is attached to the block previously placed in the archive, creating a solid IT structure that is the so-called block chain. Just like the DLT, the Blockchain Master Book has the characteristic of being a synchronized database, which means that the archives present in all nodes of the network are identical and are instantly updated with each new insertion. In addition, the Master Book present in the nodes is public, that is, it is available to anyone through the internet and an appropriate application. Another common feature with the DLT is the freedom, for each node, to be able to acquire information or perform transactions. Each node can also update the Master Book after properly reaching the network's consent. This is the phase that differentiates the Blockchain

[6] Alan T. Norman, Everyhting about the Blockchain technology

Master from Distributed Ledger Technology: Each DLT Node has the ability to collect information or execute a transaction and verify it on its own. Upon successful auditing, the transaction or information, complete with the check performed, must be submitted for approval by the remaining nodes in the network. If the majority of them agree, the proposing node has reached consensus for the work performed and can add the transaction or information to the Ledger. Blockchain, to raise its level of cyber security, has created a computer architecture that handles only digital strings of defined and standardized length called blockage. For this reason, when a Blockchain node rives information or executes a transaction, which digitally constitutes a string of variable length depending on its contents, it shares it with the other nodes. This string is added to other similar strings until it reaches standard length, that is, up to a block. At this point, the entire block is subject to the simultaneous verification of all nodes. The first node that reaches the control algorithm solution gets verification and submits its work to the approval of the other nodes. If the solution is accepted by the other nodes, the consent for that block is reached and the solver node after the encryption phase and after the time stamp (which is required to determine transaction history) and the hash, adds the block to the Ledger. The hash is a code that contains the index and location of all the information contained in the block, identifies the block itself, and has a function that allows it to connect to the block previously placed in the store. When the Block becomes part of the block chain all the

information contained within it is virtually immutable, unchangeable and secure and can be accessed by any user of the internet via the internet via special internet Application. The rules that allow verification and consensus are established and shared by all nodes of the DTL or Blockchain network and constitute their respective governances.

### 1.4 The Consent: Blockchain Permissioned Or Permissionless

The distributed ledger is a distributed store, the more in detail it is a store replicated at the same time across all nodes of a network but without control over the quality of the information stored. Distributed Ledger Technology (DTL) is an archive distributed across all nodes of a peer-to-peer network, also an identical copy across all nodes, but more evolved than the distributed ledger as it has a governance, algorithms, and hardware capability. able to reach consensus between nodes. Distributed Ledger Technology is a great innovation because it combines the logic of the replicated store on each node with the validation of information or transactions before it is placed on the archive[7]. The internet of values is traced. Consensus management models (control, validation, encryption) define a substantial difference between Distributed Ledger Technology of type Public and Distributed Ledger Technology of the Private type, which are defined as the following specified: - permissionless (without permissions) when there is no

[7] Umit Hacioglu, Ebook: Digital Business strategies in Blockchains ecosystems (pag.68)

special authority that can restrict or deny permission to participate in the transaction control and update the register; - permissioned type when defining a governance that assigns to a subject, or more than one, control of the application of the rules defined by governance and also the update of the Master Book. The evolution of the DTL is related to the grouping phase of transactions in blocks that, having reached consensus, are inserted in the chain that leads to the actual definition of the Blockchain. Every new block of transactions, as we have already seen, to be added to the Blockchain must be subjected to the analysis process, must reach consensus and be encrypted. This process requires a great deal of processing power, from a hardware point of view, as it is implemented through complex mathematical algorithms whose solution represents validation. Acceptance of validation by other nodes represents consent, and this process is called mining and is acquitted by miners. The expensive commitment of the miners is remunerated and incentivised in a different way according to the different organization of the Blockchain network between public and private. The role of these figures is similar to that used in Distributed Ledger Technology, and can be described as follows: - in private or permitted Blockchain networks the role of miner is played by one or more authorized nodes, depending on the governance studied on the purposes that the company intends to pursue and defined by the authority that activates the Blockchain itself; - in public Blockchain networks or permissionless each node may decide to play the role of miner.

Network governance defines how and quantify the miner's remuneration. In most cases it is the first miner that solves the mathematical problem to be remunerated. Solving the mathematical problem means verifying that all the information or transactions contained in a block are correct, doing this, the miner validates the block. Consensus is reached when the other miners share the solution reached, this phase takes place in the following way: the miner who first solved the mathematical problem provides the other miners with evidence of his work which is called Proof of Work. If other miners accept proof of work, reaches consensus on the blockade. At this point the block is added to the Blockchain chain and the solver miner is rewarded with the sum of the transaction fees contained in the block. Blockchain permissioned companies fail to undermine the transparency and security characteristics of blockchain, while formulating a purpose governance that ensures, to companies or banks that own the network, to pursue the purposes for the Blockchain itself has been implemented

## 1.5 Blockchain Immutable and Secure

The security feature of blockchain information retention is very important and is primarily determined by the simultaneous presence of the entire archive in all network nodes[8]. A possible delinquent attempt to tamper with data, to be successful, should take place at the same time on all copies of the ledger and this

[8] OECD Blockchain Primer pdf: https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf

operation is virtually impossible, especially in extended networks. Conservation security is also based on the already introduced concept of time stamp. It contributes to the modification of the information by anchoring any specific information at exactly the time it was archived. Associating each file change with the timestamp of the moment when the change takes place prevents any alteration of the information in the archive as it would also change the timestamp, making it different from the original. In more detail, the timestamp is a sequence of immutable characters that uniquely correspond to the date and time when the document is placed in the archive. The application of the timestamp to the computer document is called time stamping and in the case of Blockchain, which recognizes the modification ness of the document link – time stamping and the same time stamp, the date and time associated from the system to the document is legally recognized.

### 1.6 The Double Spending Problem

Digital transformation, as defined as the advent of digitalization, has radically changed the industry, the way of life of man raising its quality[9]. It also marked the beginning of an intangible world in which the reproduction of an asset or service, such as a song or software, has become simple and very cheap. The industry had to adapt to these innovations and, above all, it was necessary to address the

[9] Consulted on 04.11.2019: https://www.mycryptopedia.com/double-spending-explained/

introduction of a strong limit in the control of duplication that allows to circumvent copyrights as is often the case for the categories of goods mentioned above. This heavy limit that also involves the scope of digital coins, assuming the definition of double spending, introduces a criticality in the nascent world of cryptocurrencies that would lose all kind of participation in fear of incurring scams. The developers have found the solution of double spending and consists of defining a unique identity of the coin. Encryption, used in all systems that manage blockchain-based digital coins, allows you to manage the identity of the coin using a specific code called ID. The ID code of each coin contains its first and last name, its history with all transactions in which it was used by switching from beneficiary to beneficiary. Blockchain is an important tool that can be used to control many industrial chains such as automobile, food, fashion and livestock. This control can be implemented using the concept of the history of a coin, as described above, turning it into the history of a food product, an object, a spare part, a farm animal, a bag, etc. A tomato, for example, can tell its entire story, starting with the place and the way it was cultivated, at the time and the way of harvesting, storing, transporting, packaging or processing and again of the times and storage and transport until you arrive on the restaurant table or on the retailer's counter. In view of the fact that, in the Blockchain context, the information acquired by nodes after approval by the network and storage, the story becomes immutable and accessible to all, it is evident how such technology leads to a

change of knowledge consumers and thus a sure improvement in performance and entrepreneurial mindset. Blockchain, therefore, does not solve only double spending, that is, the duplication issues inherent in virtual currency, but also solves those related to the unique and secure identity, the traceability of any object or product and therefore introduces an epochal innovation that starts from the internet of information leads us to the Internet of values and transactions.

### 1.7 Blockchain's Logic

Blockchain logic has evolved over time according to new employment prospects. Blockchain 1.0 has been designed to meet all the needs related to the management of Bitcoin and the wallet[10]. More generally we can say that it has been specialized for the management of the cryptocurrency and therefore has a protocol that satisfies the exchange and custody of the virtual money owned by the participants in the network. A step forward in Blockchain technology was registered in Blockchain 2.0 as it involved many sectors, allowing the transfer of any kind well material or intangible. The decentralized register characteristic of this phase, in fact, could manage any type of contract and changes of ownership in the entirety of procedures. There have been many applications, and a non-exhaustive list can be: the register of vehicles, licenses commercial, intellectual property documents, contracts between individuals and insurance companies. Blockchain 2.0 has also

[10] Mauro Bellini, 2018 : Blockchain and Bitcoin

innovated the relationship between the public administration and the citizen in numerous cases concerning rights (vote, possession, etc.) and documents confirming driver's license, identity card, birth certificates, marriage, ownership real estate, etc., then for physical assets and intangible assets. Blockchain 3.0 has gone beyond smart contracts and the management of the relationship between Public Administration and citizens involving the entire industry while maintaining its ability to redesign services and standards in them. At this stage, Blockchain was able to use a digital ecosystem, created in parallel with the evolution of the Blockchain itself, allowing it to introduce a new organizational model that involves many sectors: automotive, food, telecommunications, as well as the public administration. Blockchain, in this development phase, sees interactions consisting of a value as if they were economic transactions and is therefore able to manage them and record them in the ledger. The logical model is based on the digital signature and timestamp association. The digital signature certainly identifies the sender and the recipient in any type of message, while the timestamp linked to a set of validated messages, allows their registration in the ledger of all nodes of the network and made irreversible. The transactions are therefore treated in accordance with the logic of the blockchain and are therefore confirmed by the network, through the process of distributed consent, a process that guarantees the date and time of the consensus itself and the neutrality of the Network.

## 1.8 Blockchain Features

The features of blockchain we have already encountered and are summarized and explained below: Reliability: the logic of the Blockchain provides for having an identical copy of the book each node in its network, remembering that each network participant is a node. This ensures the integrity of the distributed ledger if the copy on a node is corrupted; this feature becomes all the more robust the more extensive the network, in detail we can say that the more numerous the nodes the more reliable the blockchain network.

**Transparency**: Blockchain logic states that any information or transaction, along with all the others that make up the standard block, after validation by a node and the achievement of the network's consent, is included in the archive. From this point on, this information or transaction can be accessed by any internet user and the widest transparency[11].

**Convenience**: Blockchain logic is that each node can execute a transaction or collect information. This means that, whatever the interaction dealt with by the node, this will happen without the interest of intermediaries, as could be the banks for financial transactions, with the beneficial result of having no unnecessary expenses and therefore being more Convenient.

[11] Srinivas Mahankali, 2019: Blockchain the Untold story

**Solidity:** the IT structure of the Blockchain expects any information or transition acquired from a node to be assembled into a block; this means that the information in its form of digital strip, with function length of its contents, is associated with other strings until it constructs a string of standard length, called block. The infrastructure architecture of the Blockchain is developed on this standard string or block. The block, as we have already said, is marked by both a timestamp that identifies exactly the date and time when the block was validated; It is from another code called Hash that identifies the block, it contains the index of all the information contained in the block and establishes the link with the block of the chain to which it will be docked. All of these constraints do not allow information tampering and give the block exceptional it solidity.

**Irrevocability**: the characteristics of the block, invoked in the solidity characteristic, constrain each information to the time (date and time) at which it was recorded and to the structure of the chain, therefore, the system, for all the information stored, only allows consultation but makes it impossible to steal information just as it makes it impossible to make any change on the same archived document; these properties determine the feature of irrevocability.

**Digitality**: Blockchain by its very nature lives in a digital ecosystem; Blockchain in this ecosystem satisfies many areas of application by extending its scope with the help of equally advanced digital technologies, such as the Internet of Things

which allows sensors to detect information directly from the field and, without intermediaries, transmit them to the Blockchain which makes them no longer manipulable and therefore no longer at the service of lawlessness.

### 1.9 The Permissioned Ledger

ledger and a variant of the permissionless ledger that respects the permissionless ledger that loses control by all nodes, entrusting control only to some as trusted. In addition, it has a Governance that has rules of purpose although shared with the actors of the network[12]. The ledger is distributed and has the same characteristics as that of DTL and Blockchain. The structure described immediately suggests that the permissioned ledger is carried out with a purpose and in particular to coordinate and control all the phases of a supply chain; the permissioned ledger is all the more useful the more complex and articulate the supply chain. The most advanced permission ledger is the one based on Blockchain technology and has already been used by large companies and institutions. You can see that the structure of the permission ledger bears a resemblance to that of the central ledger, with regard to centralized governance, but with the substantial difference that in the central ledger governance is realized central authority while in the permissioned ledger governance is built with the contribution and sharing of all the actors in the network. All actors in the supply chain will access the network to

[12] David Lee Kuoo,2018: Handbook on Blockchain, Digital Finance and inclusion (pag.307)

enter the data that is the result of the processes they carry out and to acquire information, inserted into the network by other actors, and necessary for their activities, in addition to the possibility of viewing the ledger. The update of the ledger, on the other hand, is done only through authorized nodes with a methodology similar to that provided by Blockchain. Information collected by any node, grouped in blocks, will only be stored after authorized nodes have checked, validated, and reached consensus, according to governance rules. The information stored, that is, added in blocks to the chain, in the cases described above is visible to the whole world of the internet, in this case, instead, in the consideration that the permission ledger conveys data related to an industrial supply chain, that could belong to the protection of the specificity of the product, governance will also regulate the visibility of archived data by the internet and each node. The permissioned Blockchain is based on four elements: Infrastructure: we have seen the Blockchain allowed to be born to pursue an industrial purpose common to a group of actors who, in general, make up the entire supply chain of a product. The infrastructure, therefore, in addition to technologically meeting the requirements that will make it efficient for the purpose, must be secure, that is, it must be impenetrable to strangers.

Ecosystem: Blockchain permissioned, as seen above, interconnects numerous companies that together make up the supply chain. Each of them encompasses a

node, through which the company has a continuous interaction with the other nodes, that is, a two-way exchange of data aimed at coordinating and controlling the activities of the supply chain. The whole of this is the ecosystem that will have to be studied and shared with all the actors of the complex project until the design of the Governance that represents the heart and brain of the system. Applications: Blockchain permissioned, as seen above, is born with a specific purpose and, therefore, each has specificity such as to make it also very different from other experiences. This implies that at the project stage a very important interaction is needed between digital hardware and software specialists and all the actors in the supply chain who will use the network for the common purpose in order to achieve an effective meeting point between the industry needs and the needs of digitalization.

Governance: Governance in Blockchain permissioned is the heart and brain of the system and must, already at the project stage, provide for all the rules that will manage interactions, controls and permissions on the network to ensure the a

**1.10 Smart Property**

The blockchain can be used for any form of register, inventory and exchange of assets, including all areas of finance, economics and money, hard assets (physical properties), intangible assets (votes, ideas, reputation, intention, data on health

and information)[13]. Use blockchain technology in this way, allows you to open many functional applications through all segments of business involved in money, marketing and financial transactions. The property encoded via blockchain become smart properties that are negotiable via smart contracts.

The general concept of a smart property is the notion of dealing with all properties in blockchain-based models. The property could be a hard one physical world assets such as a home, car, bicycle or a computer, or an intangible asset such as shares, reservations or copyright (such as books, music, illustrations). Some assets can be registered on the blockchain, therefore their ownership can be controlled by anyone with the private key, so the owner can sell the assets transferring the private key to the other party. The smart properties, therefore, are properties whose ownership is controlled through the blockchain, using contracts subject to existing law. For example, a pre-established smart contract may automatically transfer ownership of a vehicle from the company lender to the individual owner when all the loan payments are been done. The key idea of a smart property is to control ownership and access to a asset having registered it as a digital asset on the blockchain and having access to the private key. In some cases, the hard assets of the physical world could, literally enough, to be controlled with the blockchain. Technology blockchain offers the ability to reinvent identity

[13] Melanie Swan, 2015:Blockchain a Blueprint for new Economy

authentication and access safe in ways that are much more flexible and demand-oriented on time real compared to what is currently possible, elegantly integrating them hardware technologies of the physical world with digital software based technologies on the Internet.

The smart property contracted with the blockchain is a new type of concept. We we are not used to having cryptographically and self-defined property rights applied by codes. The code is self-applied by technical infrastructure in the meaning that it is intended to operate on the basis of the underlying code and cannot deviate. Blockchain-based smart properties therefore contemplate possibility of a trust less system, global asset management e decentralized as well as cryptographically organized assets. The trust less feature of blockchain technology is a factor key in the context of smart property and smart contracts, in fact it allows smart properties to be traded without the need to trust third parts. This reduces fraud and brokerage fees, but also allows carrying out a large amount of transactions that otherwise would not they could never have been concluded, because the parts don't need to get to know each other and trust each other. For example, it is made possible for subjects in different countries to lend money on the internet, using a property of collateral borrower: this should make the market more competitive loans and also less expensive loans. Also there is the possibility that smart contracts executed in the trust less network could go through

minor disputes. Contract disputes in the US (44%) and UK (57%) count greater number of disputes that could be avoided with greater precision at the time of exposure of the agreement, or with a mechanism automatic execution. In relation to this, as theoretician Nick Szabo points out legal of cryptocurrencies and smart contracts, is the general problem irrational human decision making, which could be improved with an automated mechanism like smart contracts.

### 1.11 Blockchain And Smart Contract

The idea of building a smart contract was born after 1970 but the technology with the right skills to develop this idea was not reached until after 1990. The first smart contracts developed were simple and essential, and were made to initiate mass computerization; In fact, they were used to allow the use of software on the basis of the payment of the relevant license, and then to ban its use after a contractually expected time frame corresponding to the duration of the license paid. The conventional contract and the smart contract from the legal point of view are identical, that is, both in form and content must comply with the laws in force; In addition, the terms and possible actions a leading from the contract apply in both. The smart contract is the digital code transcription of a conventional contract with the same and identical contents and aims to automatically execute the contract; In detail, it must be able to digitally detect the realm of contractual conditions and in this situation perform, always digitally, the actions that the

contract provides. The smart contract[14], in practice, is the automatic execution of a code that detects and relates data, executing commands when conditions are in place. The critical issues on which to focus on the compilation phase of a smart contract are: the transformation into code of the contractual will of the parties; code size; certification of the source of the data to be detected; certification of the read mode. The smart contract has reached its maturity of execution only with the development of the Blockchain.

### 1.12 Token And Ico: What Are And Its Limits

The token and the ICO are two ingenious tools[15], created within the Blockchain world, capable of creating new business models but which to date lack the necessary regulatory support that guarantees certainty of the right acquired by the purchase of these instruments. The token is a digital information inserted into the Blockchain, with all the very important features insured by that technology and previously illustrated, which represents a unique form of right acquired by the user, such as the ownership of an asset or access to a service. Every good, product and service can be turned into tokenization. Through specific contracts, the relevant tokens can be sold by the title, in the Blockchain field, to finance other initiatives. The Initial Coin Offering (ICO), on the other hand, represents a new token that corresponds to a bond or share that an entrepreneur offers for a specific

[14] Larry A. DiMatteo, 2019: The Cambridge Handbook of Smart contracts
[15] Vincent Hale,2018: Launch an Ico and Token Crowsdale

project to be realized. The development of the project, in fact, will take place with the help of the financing obtained through the sale of these tokens, which investors will decide to buy believing in the good end of the project itself. The token for an ICO can also be associated with the service access right developed by the project. The lack of legislation that recognizes and regulates the right of ownership linked to a token, to date, it does not allow the development deserved by this innovation already mature for the market. In fact, 2017 has been a strong enthusiasm for the ICO but after some scams, practically unpunishable, in 2018 there was the inevitable decline and intervention of regulators to protect investors. A strong restriction on the use of tokens for regulatory deficiency is also manifested when the token represents a property right not currently legally recognized.

### 1.13 The Blockchain Bitcoin

The Bitcoin phenomenon, a digital currency not issued by a central bank, exploded throughout the world downstream from the great financial crisis of 2009, made Blockchain technology known. The Bitcoin network, which is based on the Blockchain and is owned by the same participants in the network, is able to issue digital currency and can allow its exchange over the internet and an application, issued by the same inventor of Bitcoin. This app was made open

source by its inventor Satoshi Nakamoto[16] and allows exchanges without any brokerage. Bitcoin has introduced major changes that, given the lack of adequate legal support and a strong structure in defense of the anonymity of the user, has allowed its use in financing of illegal activities and trades in the deep-web. The technology supporting bitcoin to date has made further steps forward reaching a satisfactory maturity while regulatory support is still virtually nil but it seems that the conditions have arisen to begin a process of definition. The digital currency Bitcoin is an encrypted file and has a value corresponding to the quote that the market attributes to it, in fact, like the material coins released by central banks, it is not linked to the value of a material asset. The application that has previously been referenced, in an encrypted environment, allows the exchange of Bitcoin currency and the custody, by each user of the network, in a particular personal folder called wallet. The transfer of money from a transferee to a receiver, i.e. the execution of a transaction must necessarily refer to the two subjects but, in the Bitcoin environment, which protects the anonymity of the participants in the network, it has been found a way not to detect the identity of the two subjects by creating a Bitcoin address, linked to a public key, which can be used freely in transactions and be viewed by all. The Bitcoin address will then be tied to a wallet and the wallet to the subject through unseen and protected passages. Even as part

[16] Shatoshi Nakamoto,2019: The white Paper

of the control of a transaction, the verifying node will access the Bitcoin address, via the public key, in order to ascertain the actual ownership of the currency indicated in the transaction being verified and will not be able to view any other of the also protecting the portfolio's capital strength. The Bitcoin recipient of the transaction must have created a new Bitcoin address, equipped with a public key to indicate in the transaction, linked to his wallet, which will serve the system to allocate the bitcoins agreed upon successfully. Specifically, it is a case of reporting that a Bitcoin address can contain any amount of bitcoin. The new Bitcoins, when entered in the recipient's Bitcoin address, will be marked with the subject's private key in addition to registering in his history, the transaction just concluded. These codes will attest to the new ownership of the coin.

### 1.14 The Blockchain Ethereum

Blockchain technology has also been used in another successful project called Ethereum[17]. Ethereum, unlike the Bitcoin Blockchain, was immediately conceived as a useful platform to meet many needs, in particular it is not specifically attracted for the management of crypto currency. The characteristics of the Ethereum follow those of the public Blockchain in fact can boast a network where everyone can participate and no one can prevail over the other; the archive is immutable, shared and secure. The Ethereum system introduces the new concept

[17] Kerry Gan,2019: Unlock the Secret of Ethereum

of Distributed Computing. In practice this means that the system virtually joins all the computers participating in the network into a single large computer of superlative processing power and great reliability because it consists of the sum of a multitude of computers that ensure continuous operation. The system recognizes a quantum for network participants for the use of their own computers by rewarding it by assigning system-issued tokens called Ether. Ether tokens are used on the Ethereum network as a currency of exchange. Unlike the Bitcoin Blockchain and its evolutions, the Ethereum is a programmable platform, that is, where developers can program applications that will use the platform for its purposes. The large virtual computer of Ethereum, consisting of the sum of all the computers of the participants in the network, is called Ethereum Virtual Machine (EVM) and is made in such a way that it can be seen and used only by the platform and on this specificity founds the cybersecurity of system. By means of this large computer are performed all checks, smart contracts and developer applications are executed. Despite its strict security structure, Ethereum, in 2016, suffered a hacker attack with very serious economic and image consequences. The need to react, even quickly, to the hacker attack divided the founders of Ethereum into two factions: the purists argued that the blockchain must be immutable and the defense from hackers must be shared among the participants of the network; others, however, in the belief that the only viable solution was the change of the blockchain codes, did not want to compromise and determined the split of the

platform. The Ethereum Foundation distanced itself from the splitters who created a new Blockchain with modified codes called the Ethereum Classic. The new Ethereum Classic is a Blockchain fully compatible with the Ethereum platform with a different token issuance policy and innovations against hacker attacks. The Ethereum Foundation, on the other hand, continued to deal with the Ethereum platform in relation to its support and in carrying out research and development projects against hacking and also in various other fields with prototyped realizations. There have been many notable projects: the "Frontier network" project to improve safety and usability, the "Olympic" project to verify the solidity of the Ethereum platform with a "Stress Test", the "Serenity" project to improve the algorithm of the Consent.

# II CHAPTER

## 2. The Impact Of Blockchain On Corporate Governance

### 2.1 Corporate Governance

The blockchain, in addition to revolutionizing the way in which it can bring additional value to products in different industries, can at the same time have a impact on the business of all those who run a business. Not only managers, but also investors and auditors, as well as other stakeholders, can reaps benefits in terms of cost, speed of operations and data integrity on which their day-to-day business is based. In this third chapter we will look at what dynamics and

problems related to them will be most affected by this technology and how it will affect their processes.

### 2.2 The Corporate Voting

In the European reality, the voting process in equity companies does not suffer from particular problems due to the fact that there are typically few investors who hold large percentages of corporate capital[18]. What is different is what happens in societies outside the old continent. In fact, overseas, widespread-shareholding companies (many small shareholders) prevail. In these realities, corporate proxy voting is a very common practice for making decisions at the meeting as shareholders who hold few shares travel to attend the shareholders' meeting could cost more than earnings. stemming from that stock package. The Investor Advisory Committee has repeatedly urged the Securities and Exchange Commission to review and make efficient the system of rules on which it is based. The problems reported as most relevant are: the inaccurate list of voters, the incomplete distribution of voting rights and the voting tabulation process. Operation and benefits In this regard, implementing the blockchain in the voting system could, in fact, eliminate completely the timeframes that are currently necessary to manage the flow of information between the corporate registers and the Central Deposito Securities, managed in Italy by the company Monte

[18] Umit Hacioglu, 2019: Blockchain Economic and Financial Market Innovation

Securities S.p.A., and the asset management company. At the moment this process takes about 25 – 30 days. Achieving this goal would be possible thanks to the very structure that characterizes the blockchain, that is, distributed registers. In this way the information does not need to be sent, but is by nature accessible to everyone. Other benefits are greater transparency and accuracy. These three main objectives could be achieved, including encouraging the participation of small shareholders, thanks to the introduction of tokens. With each vote, those who are entitled to vote will receive one and when they express their preference, the token will be transmitted with a transaction. This transaction will be recorded by the blockchain and made so accessible to everyone, but without being able to be modified by anyone. Empty voting Another way you could improve assembly voting is to regulate the operation of empty voting through smart contracts. Empty voting is the case that occurs when the holder of an ordinary stock hands over his right to vote to a third party in exchange for a sum of money. This separation may be partial or total depending on the period for which the right to vote is ceded. The exchange of the vote can be facilitated by smart contracts especially in the case of partial divestment. With this application of blockchain, one could either automate the actual transition of the right to vote from yielder to buyer, only and exclusively, for the contractually provided period of time, and impose constraints in the use of voting and to be able to prevent any default or, alternatively, to sanction the party that has violated the contract, always completely automatically.

The transparency of the blockchain by definition could also give more value to the action as it will be able to base its assessments on complete and updated data in real time. Finally, both management and regulators can acquire information to help monitor the purchase operation.

### 2.3 Agency Theory

Agency theory seeks to optimize contractual relationships between ownership and managers of a company. In particular, efforts are made to prevent agents from pursuing personal objectives rather than for the corporate good because of the inability of all members to participate in decisions. That's the problem. The practices in force today are based on theories, purely by Jensen and Meckling, which actually find effects that are not fully satisfactory. Agency costs cannot be removed in any way except by acting radically on the structure of delegation with which the manager is appointed. The agency costs are mainly two: - Surveillance costs; Incentive costs. Blockchain can also be used for this purpose by creating a sub-optimal situation given thanks to the characteristics of transparency and trust that distinguish it. The reduction in agency costs would directly benefit not only shareholders, with particular reference to smaller ones who often do not have the convenience of investing in management control systems, but also for the benefit of the same Company. This is because it invests considerable resources in the annual general meeting of shareholders, which theoretically aims to offer

shareholders an opportunity to monitor the managers who run their own company. The functions of this body are mainly two: providing information and making decisions. It is easy to understand, therefore, how it is possible to reduce agency costs only by intervening directly on the assembly body. Unfortunately, however, the same issues are always touched on in the assembly and that they do not offer enough data to monitor the work of managers in a very clear way. In addition, the corporate functioning is increasingly complex and dynamic, while the issues established by the law to be discussed in the assembly have not been updated for too many years. The whole thing can be read as a waste of time and money for everyone. The inadequacy of the assembly to make decisions can be explained by a brief example: co-optation. According to this practice, in the event of the resignation of a board member, the board may appoint a successor which must then be approved by the next shareholders' meeting. Sometimes co-opted directors resign even before their appointment was validated by the shareholders' meeting. This is a paradox that describes the problems related to the decision-making power of the assembly body. Blockchain is the right tool to offer the opportunity for all members, regardless of their size, to take part in decision-making power very easily and very frequently. This also reduces the organisational costs that companies have to pay for assemblies and increases the speed and leanness of decision-making.

## 2.4 Administration

Current administrative systems are centralized. This means that each part of the same transaction creates an accounting write on its registers independent of that of its counterpart[19]. This leads to a phenomenon of duplication of the writings, as well as the possibility of writing inconsistent data, i.e. errors – intentional and unintentional – and inconsistencies between the two accounting registers. Also thanks to the experience gained during an internship in the administration area of a medium-sized company, I can say that it is really difficult to come to the head of a mistake in a writing and make ends meet again; and this takes a lot of time and resources. Using blockchain could increase the efficiency of the system by establishing a single distributed ledger in which to record all transactions with a single accounting write accessible to all counterparties. This information can also be viewed by other appropriately authorised external actors including auditors, tax authorities, banks, the judiciary and the whole of the Public Administration in general. Another advantage of using blockchain in the administrative sphere is that of the immutability of data. This feature has already been widely discussed in the first chapter. In fact, once entered and certified, accounting writes are no longer editable due to the inability to manipulate blocks (time stamp tamperproof). In addition, by applying the blockchain to the corporate

[19] Consulted on 18.10.2019: https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype.pdf

administrative system, the writes can only be recorded according to the date of t[20]he transaction, thus following a financial principle. This system is called real time accounting. Accounting methods such as Accurals Earning Management [21](AEM) would therefore no longer apply whereby revenues must be recorded by imputing them to the period in which they relate and not to the time when the money is actually perceived. These practices are dangerous by opening up a number of possibilities for misleading reading of the budget reports. In addition to a reduction in the time and cost associated with the process of creating accounting structures, the use of blockchain gives a greater degree of security to the company's writings that can only increase the trust stakeholders towards society itself and, to see it in a broader perspective, also the system in general.

### 2.5 Accounts Review

What is contained in the previous paragraph has immediate repercussions and links also with the activities of the auditors. These figures are of third parties (called legal auditors) who work to certify a company's accounts, as required by law, in order to protect the market and all those who make investment decisions

[20] Definition Investopedia: "Earnings management is the use of accounting techniques to produce financial statements that present an overly positive view of a company's business activities and financial position"

based on accounting data Company. Their main activity is to ensure that the budget is drawn up in accordance with national and international accounting standards. In this regard, taking advantage of the concept of real time accounting, there will no longer be the need to have the accounting data certified by an external entity as they will be objective and unquestionable for the structure with which an administrative platform blockchain-based is well-founded. Another task for auditors is to supervise transactions with related parties. In particular, they are the operations by which the parties are in potential conflict of interest between them. The auditor must acquire sufficient evidence to certify that this type of transaction has been carried out, and subsequently represented in the budget, following all the requirements of the law to ensure that they take place under market conditions . With the introduction of a blockchain-based system, the need to supervise transactions between related parties would also be diminished. With this in mind, transactions would be stored on distributed registers and therefore all those who have the right to them could very easily identify the suspicious ones, i.e. those that take place on more convenient terms than the market standards. We can therefore conclude that there will be a real change in the tasks of auditors. We will move from the current role of assessing the correctness of accounting matches to that of responsibility for the proper functioning and proper reliability, effectiveness and efficiency of the systems on which the verification is carried out in a completely Automatic.

## 2.6 Fusions And Acquisitions

The process that leads one company to merge or make acquisitions with another is so onerous that many actors are discouraged by mere thought, especially if they are small and medium-sized enterprises. All this to the detriment of the fact that these practices can bring real benefits to both parties. The first step in carrying out and completing an M&A[22] transaction is the complete review by the potential buyer of all documents and facts concerning a particular branch or the entire company. All this takes place in the so-called data room or that room made available by the seller with all the practices of interest. This place was physical until a few years ago, but with computerization it was, of course, digitized. The data room must by definition be a very safe and controlled place because it contains a lot of sensitive data of a company. Although companies have been created to create digital and secure data rooms, among which we can mention Ideals, Intralinks and Merrill, there are still several dangers that can arise at this very delicate stage. Among the most important we can mention: - Difficulty of use; - Platform cost, - Possibility of errors, caused by the absence of automatic data entry process; - It is possible to understand many versions of a single document, so you can analyze a file that is actually obsolete; - Lack of summary prospectuses, this is because the data room is simply an archive comprising all the

[22] Consulted on 13.12.2019: https://medium.com/tncitgroup/blockchain-and-crypto-m-a-forming-tncs-legacy-23a5269279ad

documents necessary to evaluate the transaction as they are available from the same target company. These problems are detrimental not only to the burden on the acquired company, but also to the time that the buyer has to use inefficiently to reconstruct the whole situation. Thanks to blockchain technology it would be possible to enable the parties, who have no absolute certainty of the loyalty of their counterpart, to access for a limited period of time the data they need by reading not only the current state but also to have a historical overview in a clear and unequivocal way thanks to the time stamp. This could achieve that set of goals - including: integrity, transparency, efficiency, flexibility, privacy, cybersecurity and quick understanding - that serve to ensure fast and secure processes, which the market needs for the pace now these operations take place.

### 2.7 Pre - Initial Public Offer

One of the aspects of corporate governance related to extraordinary business management is related to the initial public offering. In this area too, there are practices that can be radically revolutionized thanks to blockchain, bringing concrete benefits to its stakeholders[23]. According to a study by the Dow Jones Venture Source, it took companies in 1996 about three years to prepare the offer, compared with 8 today. We can see the detailed historical trend in the following

[23] Sympiossium Proceedings: 2018 (pag.482)

chart: The company has very strong benefits in staying as long as possible in the pre-IPO phase. The main reasons why the time has dilated are:

I. Increased costs to be incurred, as shown in the previous graph;

II. II. Regime of obligations much less intense both in terms of regulation to which we have to submit and the reporting to be produced. Both incur huge costs;

III. III. Possibility of distortion of the business project due to a weakening of the position of the founders in favour of new shareholders who change the course to achieve higher profits;

IV. IV. An already solid brand and/or financial situation for which there is no need to go on the market. However, it should also be noted that there are also downsides to staying in the pre-IPO phase, both at the expense of the company itself and current and potential investors:

I. Those who have invested large amounts of capital in the start-up phase of the company may need to recover liquidity as soon as possible and sell shares in unlisted companies is a difficult operation;

II. II. Potential investors who want to take part in the project and contribute to it economically in such a way as to accelerate its development, cannot do so because the securities are not yet on the market. Although, in this regard, it must be added that often only traditional investors are able to

buy stakes at the time of market launch, while retailers are only able to access these securities later, when the growth has already passed its peak.

III. III. The capital that the company could raise in the pre-IPO phase is limited, especially when related to that obtained from an entry into the market, and may not be sufficient to carry on the activities. Those who argue that a repeat of the financing actions could not be considered that investors' interest could be dampened due to the increasingly watering down effect of each round of participation. Through a blockchain platform, the secondary market of pre-IPoRs could be made much more liquid by introducing tokens in this area, which we have already talked about several times. Tokens are nothing more than virtual parts of the capital of real companies in the pre-IPO phase, the value of which increases as the value of the underlying company increases. These elements would bring confidence and security to a market that at present presents itself as unreliable and very illiquid. These tokens could be exchanged through a special platform that offers itself just as an intermediary between the world of cryptocurrencies and the traditional secondary market. To this must be added not only the still widespread scepticism about digital currencies, but also the fact that tokens unlike normal cryptocurrencies, such as bitcoin and ethereum, are an investment

based only on a business project and nothing yet of Concrete. This can be read as an additional risk to support. The advantage is that equity holders and pre-IPO investors have the opportunity to unlock the latent value of their shares by putting them up for sale through a special platform. This company will then sell the purchased tokens to those who have an interest in joining the capital of the same pre-IPO. This creates a winning situation for all parties thanks to the application of the blockchain. Such operations certainly have two main advantages: - Transaction costs reduced to the only fees to pay to the blockchain platform manager; - Investors do not feel "trapped" and are encouraged to invest; - Absence of any kind of statutory information requirements for secondary markets. With regard to the last point, we should not underestimate the importance of these obligations that the law currently imposes in order to protect investors. These, however, can access the information they need to make the decision to invest or not thanks to the opportunities offered by the blockchain that we have already discussed.

**2.8 Whistleblowing**

A whistleblower is a figure that we can define as a whistleblower of wrongdoing. In fact, he is the one who, in addition to carrying out his work, intends to research and report the implementation of illegal, unethical or simply incorrectly practiced

activities within the public or private organization in which he lends his work. Theoretically[24], these people are incentivized to bring out these practices through a remuneration system. This person is, in fact, reserved a percentage of the consideration that the or the culprits must pay into the coffers of the damaged organization. On a practical level, however, those who wish to denounce often have fears of possible repercussions and therefore prefer not to do so. The main risks to which whistleblowers expose themselves, given a brief analysis of real cases found on the web, are the following: - Retaliation by their managers: those who bring out the problems may find themselves in a hostile work environment, or, in cases worse, a dismissal for false causes. There are laws to protect the subject but they have proved historically ineffective; - Bad references: the company in which the irregularity was taking place could in fact spread the word that the subject has denounced the company by making sure that other companies are reluctant to nominate him for a job; - Legal consequences: a whistleblower may also be involved in the sentence if deemed complicit in the crime. This happens when, for example, at first this employee had taken part in the wrongdoing and only after decided to confess the whole thing. The amount to be paid for legal costs and compensation may be higher than the gain and therefore also from a financial point of view may not be convenient; - Professional

[24] Rodrigo da Rosa Righi, 2019: Blockchain Technology for industry 4.0

violations: In some cases, the confession may violate a contract or a professional obligation. The consequence for these individuals could be a subpoena. The law, still with strong differences from state to state, protects little who finds courage and denunciation; the consequences are sometimes very serious and it has also happened, in particular cases, that they have been killed at trial. The intervention of blockchain technology, even in this important aspect of corporate life, could bring benefits. In fact, it could take advantage of the characteristic of anonymity that blockchain guarantees, just as it already does in the context of transactions made with bitcoins, in which it is impossible to identify the identity of the subjects who make the exchange of money. Equating a bitcoin transaction with a whistleblower's complaint could provide the following benefits: - Improved level of protection for those who report; - Track the progress of the verification process on the authenticity of the facts told; - Ability to trace the identity of all those who have accessed the information by being able to also track any attacks on the system. The further step to protect them is the possibility of receiving the financial premium provided for the complaint in bitcoin, guaranteeing even at this stage the anonymity of the whistleblower.

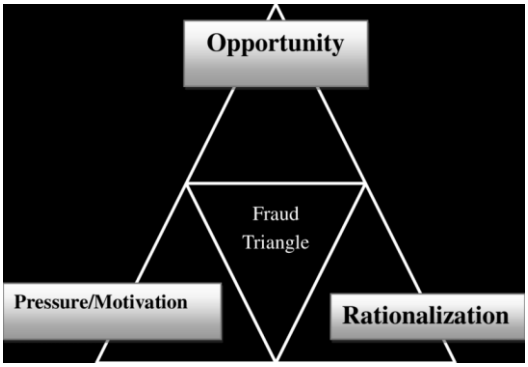
## III CHAPTER

### 3. Definition of Fraud

Fraud has its roots in the distant past. Over the centuries, it has evolved, invigorated and has taken on even more refined shapes, devising scam systems in more subtle and elaborate ways, difficult to unmask before the fait accompli. A first definition of fraud may be that provided by the U.S Legal System *as a broad legal term referring to dishonest acts that intentionally use deception to illegally deprive another person or entity of money, property, or legal rights*. The concept of fraud can be understood in three different ways: a) an act intended to take advantage of other's trust(b) an act aimed at harming others, (c) an act aimed at evading the law[25]. However, fraud theories tried to explain for the longest the reason why an individual involves himself in a financial statement or any type of fraud. This theory suggests that individuals become involved as a result of the fraud triangle, explained as opportunity, pressure and rationalization. (Cressey,1953). These three elements are illustrated in the figure 1 bellow:

*Figure 1: Representation of the Fraud Triangle(Source: Cressey,1953)*

[25] Sally Ramage,2006: A Comparative Analysis of Corporate Fraud




The first element of this triangle is pressure/motivation. Pressure usually involves a financial need, although non-financial or perceived pressure, such as greed, the need of report better than the actual performance, a challenge to beat the system, or even fear can motivate fraud. These pressures don't have to be real; they simply have to seem real to the person.

The second element is opportunity. The perpetrator must believe that he or she can commit the fraud and not get caught, or if he gets caught nothing serious will happen. An example of perceived opportunity could be a CEO manipulating financial numbers and believing that the media or the shareholders will not find out, or that the problem will go away by itself (as the case we will analyse later on this paper).

The last element is rationalization, which refers to a justification for committing the fraud. Individual believes that fraud is the only solution for his problems, or is simply following the leading example of someone who commit fraud before him and suffered minor consequences.

### 3.1 Fraud throughout history

The birth of fraud, could be traced back to birth of the economy; ever since men started trading various products, some of them also had the instinct to do it in an illicit, unethical, "illegal" way in  some sense, although this term could result *ante litteram* in a context extremely archaic in which the concept of legality and illegality is difficult interpretation. In reality the same term "economy" should not be used when speaking older than ancient Greece, since the term "economy" it would derive from the Greek and would mean "care of the house" ( *oikos*+*nòmos* ,house+norm). However, the economy in its broadest sense has existed roughly since man exists, originally in the form of simple barter. To make a profit greater from their activity men have also sought "illegal" ways, among cases reported by historiography one could for example cite that of the craftsman of Gerone, king of Syracuse; in the III-II century BC he tried to deceive the sovereign by mixing with goldnof the crown he was commissioned to make, less precious metals, however his deception was discovered by the mathematician Archimedes. It can be rightly stated, using the words of “Giorgio Nebbia” *(Bologna 1926),* who stated that since money has become the tool for measure the value of things and its possession the instrument of the measure of the prestige of men, scams have been more and more frequent in the history of mankind. Former Cicero (106- 43 BC) defined in “De Officiis” fraud as one of the main forms with which it perpetrates injustice. Throughout history there have been multiple

developments of this institution and of the mechanisms put in place to repress and punish it[26]. The most ancient and archaic frauds are what we would now call "food fraud"; this certainly does not surprise us if you think that at the time the main human activities were those related to agriculture and to the breeding and that the same trade mostly related to their products. In the Bible are reported episodes of men who falsified the weight of wheat with rigged scales (700 caC). Pliny the Elder (23 - 79 AD) in the Naturalis historia tells of how merchants adulterated spices and foods to make them more pleasing to the eye in order to incentivize people to buy them. Subsequently with the spread of culture and culture Arab customs developed a real "culture" of fraud and the fight against it, anyway that there is evidence of scientific treatises on fraud classifications and methods for shame them. In the Arab world it was originally the caliph who was in charge of the checks to maintain order and ensure respect for legality, but at a later date, on an equal footing steps were taken to develop and entangle these types of crimes to the refinement of the vigilance, therefore, around 800 AD, *hisbah* , one was established local police specifically responsible for ensuring fairness and honesty in trade and commerce markets, having the task and authority to unmask fraud, punish and repress it, checking for example the weights and measures in the markets that were the main occasions in which the

[26] Edward J. Balleisen, 2018: Fraud: An American History from Barnum to Madoff

misdeeds took place. With the industrial revolution, fraud saw its "maximum splendor"; in 1834 he came the first commission of inquiry into food fraud has been appointed. To make an account of as it was usual to pass off absolutely poor quality food for good food genuine, at the time a satirical English cartoon became famous in which one was represented a little girl asking the shop assistant for a pound of the best quality tea for kill the mice and half a hectogram of chocolate to exterminate the cockroaches. England was there home of the first law against food fraud, dated 1860, the Adulteration of Food Act. Emile Zola gave in his work *The Belly of Paris* (1873) a gruesome picture of the Parisian city from the point of view of the spread of food fraud. Only a century later than with the various journalistic inquiries and the birth of the various Consumer Associations Food fraud will see a marked slowdown, though even today it could not be said that they have completely disappeared. Not only are food frauds that have plagued history, the case has been cited of the artisan of the king of Syracuse and certainly like him there were others. Wanting to make a perhaps abrupt leap forward in time, especially in the twentieth century, fraud has actually assumed more upsetting characters, involving a growing number of people and causing more and more substantial property damage. In particular, it is just in the 1900s that the famous “Ponzi” scheme was orchestrated and implemented for the first time and had much "success" also had in the following years up to the present day. It seems that Carlo Ponzi was not the father of this scam, however the one he implemented

had a great deal resonance and made a great stir between society and the mass media of the era that was renamed with its name. Carlo Ponzi[27] was an Italian immigrant who landed, together with the indistinct multitude of immigrants who arrived in those years in the Americas, on the Canadian coast in 1903, at the age of 21. Carlo was quick to demonstrate his fraudulent nature and shortly thereafter was convicted of counterfeiting banknotes. Then, he moved to Boston where he had the diabolical idea of practicing the aforementioned scam. The fake investment which he claimed to be exceptionally profitable consisted of a kind arbitrage on the price of international stamps used by American emigrants for send letters to the countries of origin; in fact, while in America such stamps came sold at about 6 cents, in Europe their cost was about the equivalent of the sixth part, in substance Ponzi pretended to buy such stamps in European countries like Italy and the Spain and to sell them back in the United States. However, he never started such investment, but limited itself to "attracting many fish to the net" (originally the emigrants of his community) fascinated by the idea of making easy money in a short time. What Ponzi did was the basic functioning of any such scheme, which then turns out to be will deepen during the discussion, it was to involve more and more investors, remunerating the old with the money just received from the new. As can be understood, in the when there would no longer

[27] IMinds,2014: Ponzi Schemes

be new investors, the last ones left to be paid would have received nothing and the scheme would collapse. So it happened e Ponzi was sentenced to 8 years in prison in 1926, after collecting savings in a short time unsuspecting investors for $ 9 million and leaving a hole of about $ 6 million, exorbitant figures for the time.

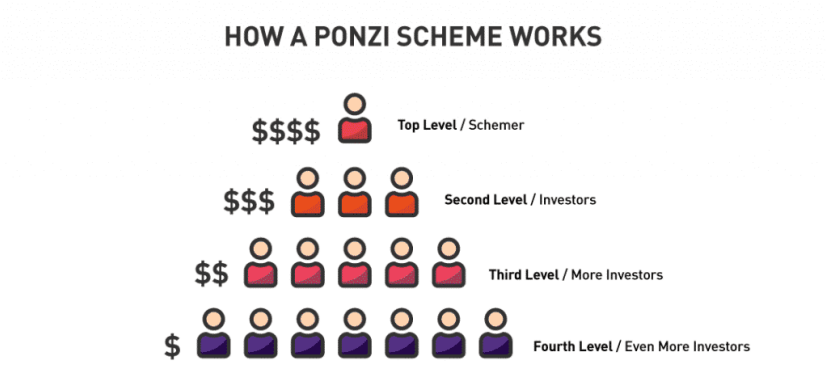
This, which is perhaps the first emblematic case of Ponzi's scheme, will find a great deal development and will be applied several times in the course of the XX and XXI century in ever new forms and each time more sophisticated. Subsequently some of them will be considered trying to

understand its dynamics on a case-by-case basis. However, one should not forget that the scheme Pyramidal described is not the only form of financial fraud implemented. In the 1900s and over the years 2000 there were multiple scandals involving both private individuals and large companies.

Furthermore, especially in recent years, with the development of the most advanced technological systems, if on the one hand, it has become easier for supervisors to uncover the misdeeds, on the other it was also easy to devise illegal plans to defraud investors; but what is the motivation behind the spread of so many cases of fraud from the 20th century onwards?

An example of how the Ponzi scheme works is illustrated in the figure 2 below:

*Figure 2: Rappresentation of how a Ponzi scheme works(Source: kucoinblog.com)*




### 3.2 The role of financial culture

The 1980s were the years of the explosion of financial culture, of the feverish mania for wanting to get rich working on Wall Street; young American offspring just Ivy League school graduates, particularly Harvard and Princeton, unscrupulous and unscrupulous, they were preparing to work in the most famous investment banks of the world. The well-being and economic boom of those years led to growth huge share market and companies hired mainly young people enterprising and not very risk averse, animated by a strong corporate and financial culture[28].

[28] Irene Finel- Honignam, 2009: A Cultural History of Finance

It is in 1983 that the director Oliver Stone made the famous film Wall Street giving fame and perhaps it could be said that even the figure of the broker Gordon Gekko could be said to be more polished than to that of the good hero Bud Fox. In fact, although Gekko turns out to be the villain of the film, the unscrupulous billionaire full of arrogance and greed, who will eventually be condemned and imprisoned for insider trading, his is the emblematic figure of a company ready to any action, to abandon any value and ethics, with a view to earning, of profit. In this sense, then, it is the financial culture that established itself in those years that it has favoured and promoted the perpetration of fraud. It almost seems to justify it where the money is success seems to be everything to aspire to. Culture is an inextricable set of circumstances, habits, education, social environment. If businesses become primarily "Money generators", then their managers are forgiven for any irregularity if finalized to do more. The incentive remuneration system itself seems to affirm that ,the higher the profits the greater the bonuses for the managers and therefore the problem of the so called "agency risk", that is of the management that takes decisions of short term risky and against the interests of the *stakeholders* themselves in order to make money more about the company. Culture in general represents a powerful weapon against fraud but at the same time he is also its accomplice. Andrew W. Lo conducted a research in 2016 analysing the main determinants of culture; these can be the environment outside,

the figure of a charismatic authority, perceived as a leader, that influences for example, the working environment in which he acts, for example, the ambition to ascend to social scale and finally economic incentives. The environment is what is most extensive mention: the places you frequent, the people, the family you belong to. An environment extremely competitive, as could be that of finance, will lead to a high ruthlessness and lack of scruples; also a leader strongly charismatic like Gordon Gekko in "Wall Street" could drive both in the good and though even in the bad, as indeed happens to the young trader Bud Fox, who lets himself be enchanted by the charm of a man who poses as God who came down to earth, strong in his social position which it occupies and its assets. It is at the same time the strong desire to emulate such a character and get what he got that could lead to same ruthlessness, inability to weigh risks wisely and to look into the long term rather than only short term, to lead towards the same results as abandonment of authentic values and justification for everything, including scams. In fact, in the film Gekko encourages young Fox with thousands of dollars' checks to get information not yet public anyway.

The graph in figure 1.1, made by Dyck, Morse and Zingales (2013) within a study on the impact of the context on financial culture, shows how the value of company market, increase the number of frauds with it in the first 5 - 6 years. However, yes can observe how the years coinciding with the succession of

the bubble burst new economy in 2001 - 2002 saw a backlog of scams. This is because in the periods following the onset of a financial crisis there is a strengthening of regulation in this area and the actions of the various supervisors. The same observation can be made to make about the number of Ponzi schemes documented by the SEC (fig. 1.2). Also in this case in the period from 2010, following the financial crisis which broke out in 2007, there is a drastic drop in the ponzi schemes implemented.

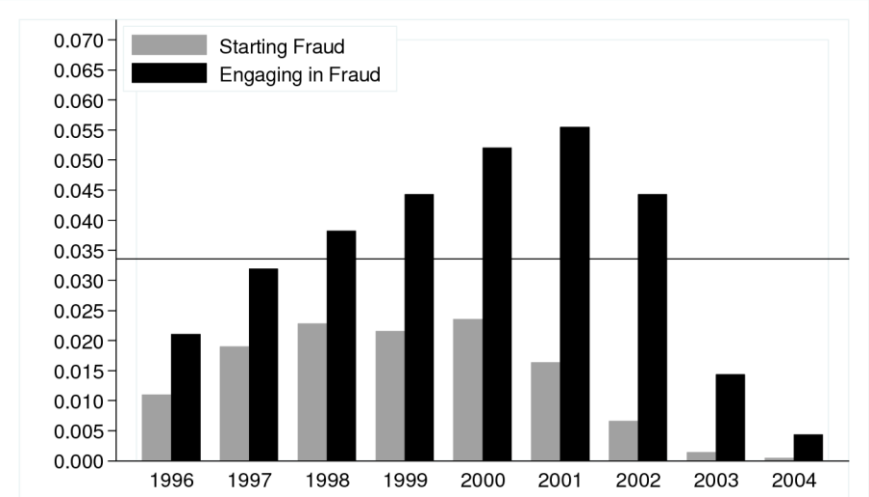



*Figure 1.1 - Estimate of the percentage of US companies involved in fraud cases (Source:Dyck, Morse and Zingales, 2013.)*

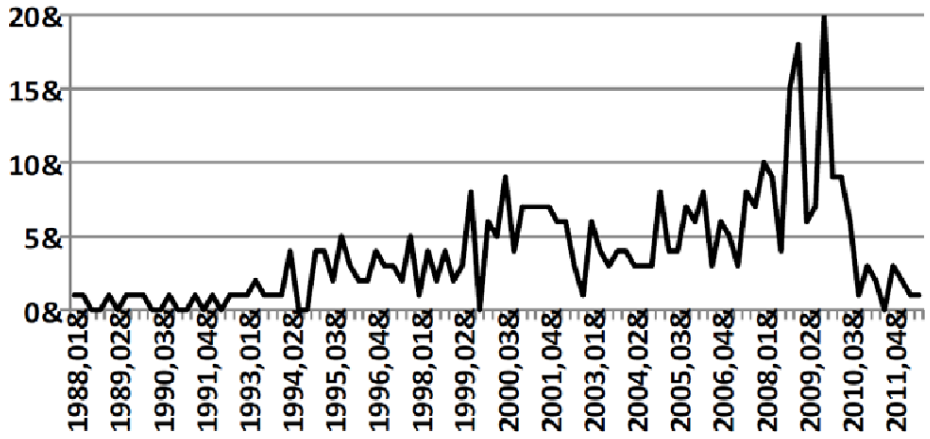



*Figure 1.2 - Trend of Ponzi schemes in the twenty years '88 -2011 (Source: Deason, Rajgopal and Waymire, 2015.)*

The Security Exchange Commission in the particular case of the United States and in general each financial supervisory body, they also have a central role in the affirmation of financial culture. They should indeed promote an ethics such as to discourage the perpetration of fraud and repress it with due penalties where necessary. Nonetheless, this is not so obvious. When in 2008 it exploded

Bernard Madoff's scandal, which will be discussed later, insinuated that the SEC did not so diligently performed his duty. Bernard Madoff was convicted of having implemented a $ 65 billion Ponzi scheme, the most conspicuous in the history of this type of fraud. Although the scandal only came to light in December 2008, it actually was from time for a certain Harry Markopolos, portfolio manager who worked for Rampart Investment Management, sent several reports of suspicious

activity about the company of Madoff to the SEC, which however never investigated, at least until the outbreak of the scandal itself. Why? Maybe not to throw alarmism and spread panic, either in this case too it could simply be a resulting bad influence from the bad financial culture prevailing at the time. The SEC itself, in order not to arouse the reaction from the media and the public, it may have ignored these reports. Like to counter excessive open-mindedness? How to fight financial fraud? Not strong personal values are enough if a whole environment is corrupt; you should apply the *SIMON* rule[29] (Select, Identify, Measure, Optimize, Notice) also to the behaviour to be taken in the business world, so as to counter the reckless risk taking, carelessness for the consequences of one's actions in the long run. Inculcating one similar education, there would also be a reduction in the various financial frauds, which instead they are still frequently perpetrated to this day, in forms that are updated and continuously modernized.

## 3.3Types of financial fraud

### 3.3.1 Fraud and *Hedge Funds*

Coinciding with the financial crises, *hedge funds* have increasingly come to the fore whose managers, following an active policy, set themselves the objective of obtaining returns absolute, not parameterised to a market benchmark. This goal is

[29]Harold Kent Baker, Greg Filbeck,2017: Hedge Funds: Structure, strategies and performances

pursued selecting *asset classes* with trends not correlated with traditional ones (shares and bonds) and activating strategies characterized by a high risk profile. In literature there are several classifications of *hedges* that could be traced to three:
a) *Macro funds* : funds that speculate on the performance of interest rates, currencies or stock markets;

b) *Arbitrage Funds* : funds that focus their activity on transactions arbitrage between different markets;

c) *Equity Hedge Funds* : funds whose business consists in the purchase with indebtedness or the short sale of shares according to the expectations on the market trend. In addition, each of the main categories presents a complex and articulated series of sub-categories of funds.

There are basically two levels of commission: the management level, relative the activity performed by the manager and performance (whose variability depends on the performance obtained by the manager, provided that it stands at a higher level than that from the previous year). In determining the management level, the mechanism of the *high-water mark*, that is the one for which the manager gets the commission of management only if it "beats" the return achieved by the fund the previous year. This could trigger a perverse mechanism that would induce fund managers to take ever-increasing risks to overcome the past level or push them to

falsify accounting records to achieve their purpose. Assuming that this is not possible the manager will opt to close the fund to open a new one later.

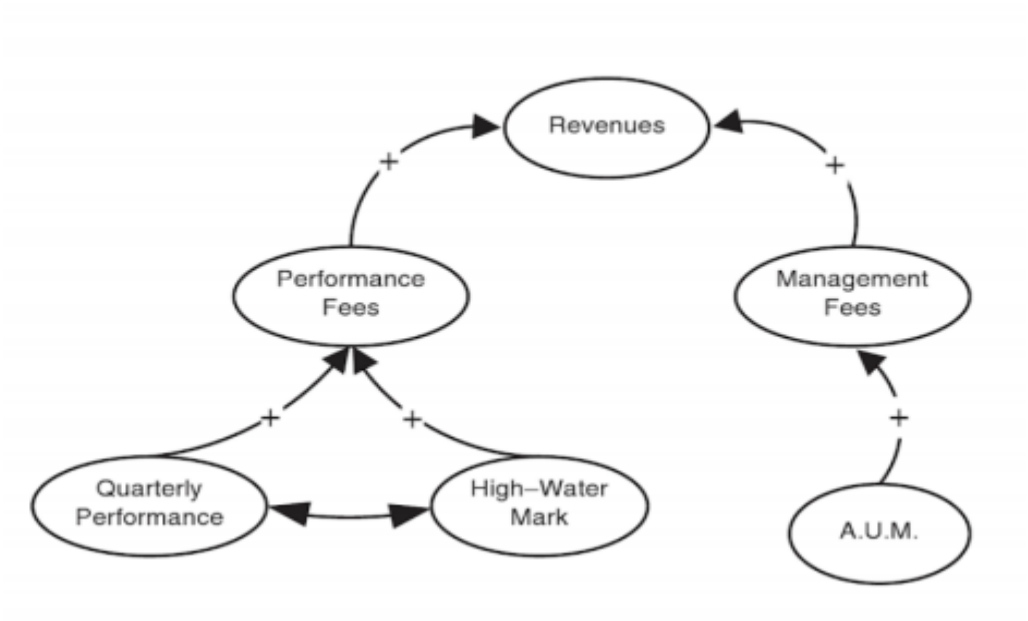



*Figure 2 - Double commission system in Hedge Funds. (Source: Johnson - The Hedge Fund Fraud Casebook, Wiley & Sons Ltd, 2010.)*

The *hedge* funds adopt, as already mentioned, various investment strategies reach the *target return* set at the beginning of each year. Each of these will present then a different degree of risk - expected return. In figure 2.1, based on the sample examined, it is clear that the profitable strategy in terms of risk - return is the BUT.

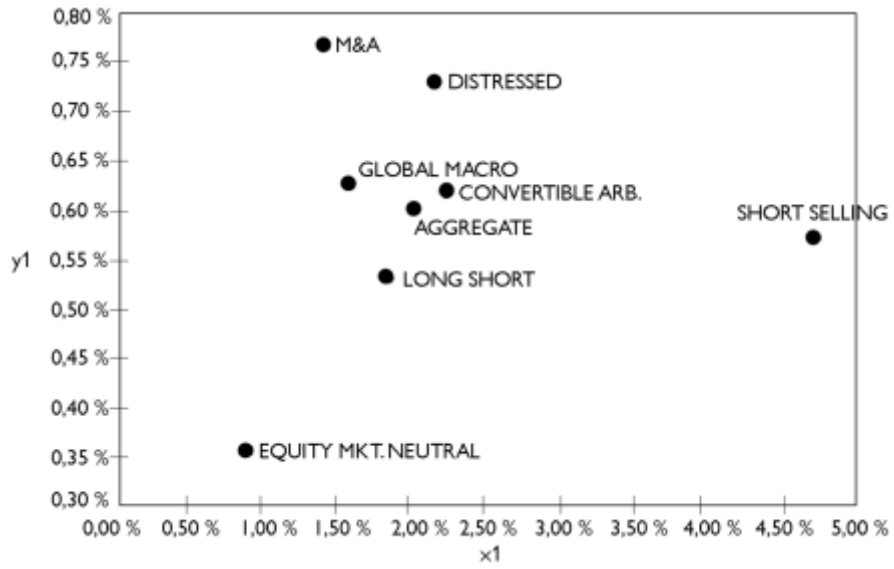



*Figure 2.1 - Relationship between standard deviation (x1) and expected return (y1). (Source: Burchi -Invest in Hedge Funds. Performance, risks, investment strategies, 2011.)*

In the *hedge* world, the most common frauds can fall into two macro categories:

a) *off* fraud *the book*, those that provide a true balance sheet representation, but one underlying illegal activity;

b) *on the book* fraud which instead tends to falsify or ad conceal the real estate situation of the fund.In general, the most common frauds are connected to the manager's desire to conceal losses, for example through a misrepresentation of statements in *offering documents* or in *reporting* documents , or through an allocation fraudulent investment opportunities.

Sometimes there are also cases of misappropriation of the fund's *assets* by the managers themselves. The problem in this area is the lack of rigid controls on the part of special supervisory fees that guarantee the reliability of the various funds and the absence a rating evaluation criterion that allows to establish its solidity. One way to predict the risk of fraud for a *hedge fund* could be to

a quantitative analysis of the returns of the funds themselves; in fact in a research conducted in 2012 (Nicolas PB Bollen and Veronika K. Pool) it has been observed that the sequence of returns could constitute a *red flag,* i.e. an alert to identify funds subjects at risk of fraud (Ponzi scheme, misappropriation of *assets* or falsifications of *performance* ). In fact, from the study in question on the returns achieved by different *hedges* American *funds* between 1994 and 2008 showed that the funds with average yields and *Sharpe* Higher *ratios* were those that had undergone SEC inspections or had undergone lawsuits from investors.

The main signs of fraud risk ( *red flags* ) are the following:

a) # *Zero* : it is a *red flag* if the probability that the fund achieves returns equal to 0 is less than 10%;

b) *Negative%:* when the percentage of achieving negative returns is less than 10%;

c) *#Pairs:* is the number of equal double returns that repeat;

d) *% Repeats:* is the percentage of equal returns that repeat over time.

Furthermore, another indicator of fraud risk could be the high serial correlation between the returns of various periods. Regression is performed to determine whether this is high or not of returns observed as follows: = + (1 -)+(1) represents the return achieved by the fund in year t; is the yieldachieved the previous year;is the value of returns adjusted to a dataset in the period t-1; it is an element of disturbance or error. It represents the correlation serial that occurs at periods of low returns, which are hidden by the managers of the funds by delaying their representation and falsifying them with previous returns. In substance if it is a positive number it is very likely in the presence of another *red flag*. The conclusions that can be drawn regarding the reliability of a fund are that in Generally there is an association between the incidence of violation and the presence of some *red flags* that they are therefore good indicators for risk measurement. Very often investors are attracted to funds that promise them high annual returns without weighting the possibility that the promise of such returns could only be "a mousetrap", in fact, we have seen how much higher returns than the sector average can be the sign of an underlying fraudulent activity, that it is a Ponzi Scheme, one misrepresentation in the financial statements, or misappropriation.

### 3.4 Ponzi and Pyramid schemes

The Ponzi scheme is one of many types of financial fraud that occur, perhaps one of the most common and practiced[30]. It owes its name to the Italian Carlo Ponzi who arrived in America in the early twentieth century, he designed a scam that earned him in 1920 $ 250,000 a day. It is divided as follows: the fraudster is usually a person apparently reliable, towards which one is instinctively induced to feel trust. On the base of its good reputation it attracts unsuspecting investors: the first ones generally belonging to his own social group (in Ponzi's case, for example, were the Boston emigrants), who they are drawn to the promise of steady and safe returns. However, the scammer is limited to repay the first investors with the capital received from the latest arrivals, allocating the previous capital raised for personal purposes. The moment new ones fail subscribers who bring new liquidity into the "fake fund", this "castle of paper" it collapses, causing severe damage to the last investors.

The elements of any successful Ponzi scheme are:

a) a fake investment strategy credible
b) , b) the promise of lavish returns,
c) c) a braggart of such strategy and such more than reliable and reassuring compensation (Ponzi was a very charismatic man who enjoyed of an excellent

[30] Books Llc,2010: Ponzi and Pyramid Schems

reputation like Bernard Madoff, former president of NASDAQ[31], who gives him 1990s to 2008 implemented a colossal scam). Ponzi schemes can then take on differences shapes and variations, one of them is *Pyramid Marketing.* The characteristics of marketing pyramidal are:

a) Sale of scarce or intangible goods and / or services

b) Recruitment of new people

c) Quick *turn over*

The functioning of this mechanism consists of a number of customers / sellers per first level, those chosen by those who start the chain, these must reach a Q number of other selling customers, where *p* represents the level number. At each new level there more and more customers / sellers will have to recruit an even larger number of people due to the exponential nature of the scheme.

This form is illegal because most of the individuals who participate in it end in order not to make any gain, on the contrary they will lose you. They believe they can get it a certain good or poor or particularly expensive service at a reduced price, so they pay for this reason, even before receiving it, those who involved them in the scheme, i.e. customers / sellers of the previous level, the latter in turn

[31] Definition Investopedia: It is a US-based stock exchange that focuses specifically on technology companies. Founded in 1971 by the National Association of Securities Dealers, its computerized systems are designed to allow efficient and transparent trading.

with the money received will succeed procure such good. The old sellers therefore leave the scheme satisfied. Now for who has taken their place, however, the task is more difficult, in fact they will have to enlist a newer customers and future sellers becoming more difficult for future entrants in the chain get good. All of this actually takes the form of a pyramid where the people who are at the top are the first "hired" than with high probabilities manage to sell the good and obtain the benefit, the more you go down the pyramid the lower the chances of obtaining the desired profit. Those who are at the base of the pyramid are generally those who will find themselves at a loss, as compared to a initial outlay will not get any good. Figure 2.2 shows the typical structure of one pyramid scheme: at the top or first level of the scheme there are 6 people, who are the initiators

of the "chain", each of these, in order to obtain the desired good, should enlist a in turn 6 other people, assuming that the people of the first level all succeed in to involve the exact number of people, it would go down to the second level where there are 36 people who in turn will have to enlist 6 people each, possibly going down on the third level and so on. It can be deduced that if for the first levels the pyramid results sustainable and the participants will be satisfied, some of those who are at the base, in this case at the twelfth level or even at slightly higher levels, could not in any way

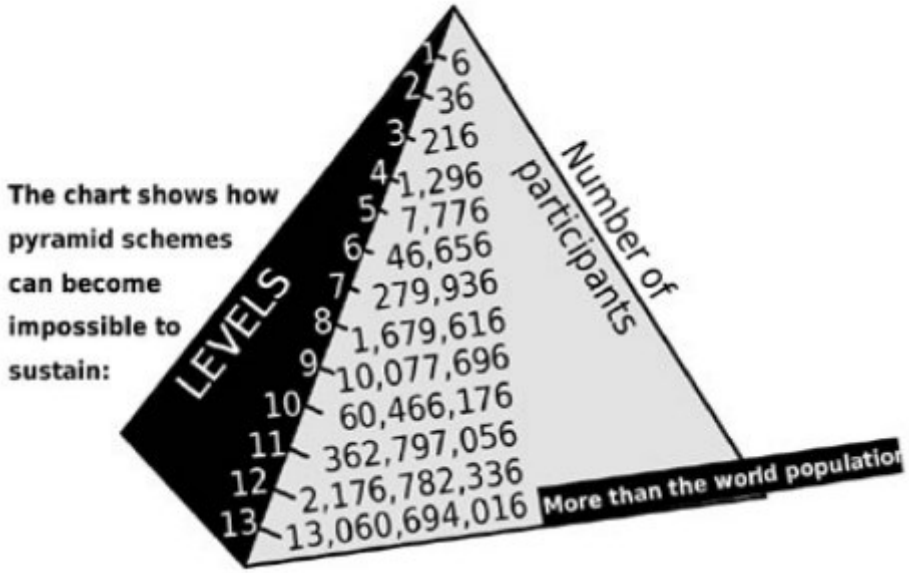



*Figure 2.2 - Typical pyramid scheme. (Source: Security and Exchange commission, US Federal Govt.)*

way to have the good or service they already paid for as it would come to a point so the world population would no longer be sufficient to absorb all the supply here I'm. In the figure at the thirteenth level there is a number of people which is equivalent to approx. double the world population. Pyramid marketing is illegal and not to be confused with the multilevel one which instead consists simply in recruiting new promoters for the sale of a product among the company's customers. The fundamental difference is that while pyramid marketing immediately requires an initial investment without no guarantee of return unless

before having involved other people in the scheme, the multilevel marketing consists in the immediate sale of the products through

the intermediation of a promoter outside the company who tries to sell the products a groups of people he knows.

### 3.5 The Misappropriation of Assets

The *misappropriation* of the *assets* of a company or entity in general consists of depletion of the company itself by another person for his own benefit or for the benefit of a third party not directly involved in the fraud. The protagonists of these fraudulent incidents may be the employees of the company, the customers themselves or other subjects external[32]. The two main cases of *misappropriation* are the subtraction of liquidity and theft of corporate assets. A research conducted in 2010 by the ACFE (Association of Certified Fraud Examiners) has shown that 85% of fraud in the past decade has occurred this area had as its object the subtraction of company liquidity, by doingbe false in the balance sheet to cover these thefts.

When dealing with *misappropriation*, the specific moment of life must also be considered of the society in which this can be perpetrated and according to it, we are in the presence of so called *skimming* or *defalcation* when the

[32] Samer Taher Mustafa,2003: Misappropriation of Assets: A Test of SAS No. 82 Risk Factors books.google.it › books

misappropriation of company *assets* occurs even before they are recorded in the financial statements. In this case the theft occurs a Upstream of the whole business process, scammers take over corporate assets that obviously they will never be recorded in the financial statements. Theft can also occur while various corporate assets are held in the company's assets, or during the process the purchase and sale of goods are made in the financial statements of purchases greater than those actually made so as to take possession of the *surplus* illegitimately gained.

In addition, corporate money theft can manifest itself in various ways: a) payments made to company name for personal purchases with invoice forgery; b) false refunds business expenses; c) registration of false cash flows to conceal the removal of money.

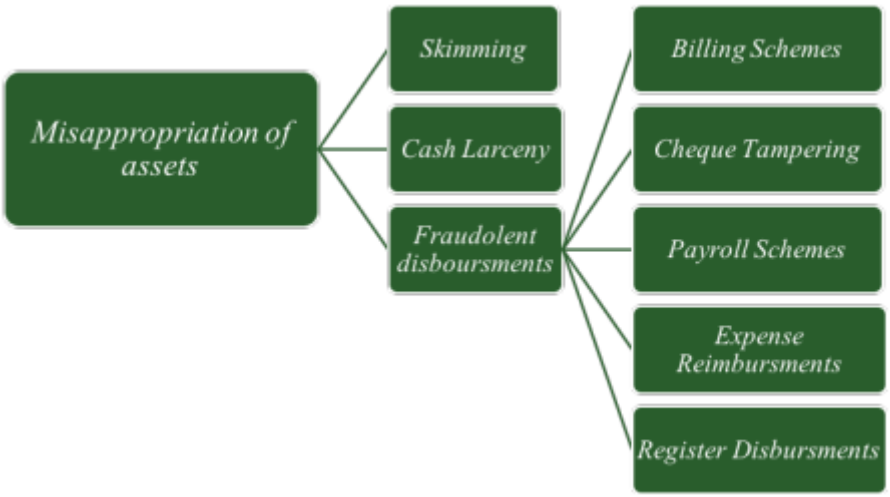



*Figure 2.1 - Tree diagram of the various types of misappropriation (Source: ACFE,2010.)*

The *misappropriation* of corporate *assets* poses a serious problem for companies;

The same research mentioned above has shown that these are subject to annual losses for a total amount of 7% of its profits due to various frauds including embezzlement. Furthermore, the collected data showed
that *misappropriation* results be the most widespread and most frequent crime among the various types of fraud that occur in professional working environment.

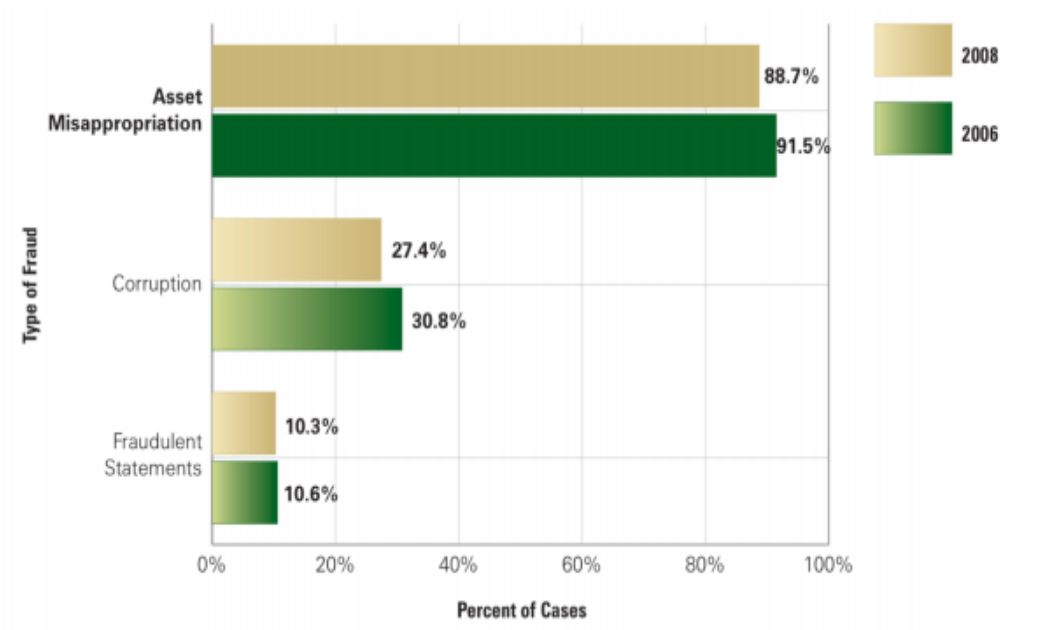



*Figure 2.2 - Occupational fraud frequency (Source: ACFE, 2010)*

To understand the seriousness of this crime and its impact on a woman's economic situation company consider the following example: a car company is the victim of a large one misappropriation scheme of, assume, $ 436 million, making accordingly reduce the net profit by the same amount, the profit margin (net profits / revenues operating) prior to losses from fraud was 10%, this implies that the auto company is expected to generate additional operating revenues of $ 4.36 billion, which implies that the company to keep its *profit margin* unchanged and eliminating the negative effect of embezzlement should be successful revenues that are ten times the cost of the fraud. Generally the protagonists of this type of

fraud are the *white collars* , those who belong to a medium-high social status and carry out professions of responsibility within the company where they work. The motivations that drive them are perception: a) an opportunity; b) of some pressure and c) of a legitimacy to perform the act.

In addition, usually those who begin to commit this crime by operating individually with the passing of time he looks for accomplices to enlist by promising them compensation or forcing them for example, with layoff threats. Misappropriation of corporate assets is a crime that affects many companies, however often these, when and if the crime is discovered, try to conceal such public opinion episodes so as not to damage the company's image by simply limiting itself to dismissal of the guilty. Companies are the first who have the responsibility of combat this phenomenon. They should equip themselves with efficient and prompt systems internal control and accounting, monitoring, information and communication. The *Internal auditing* mechanisms are indeed critical to fraud prevention, not only of *misappropriation* . A survey conducted by "KPMG in 2004" showed that, in the companies where they are present, the incidence of the various corporate scams is less. Generally the prevention of misappropriation can be implemented either warning suppliers and customers about all the company's purchasing and selling policies making it known to the employees that the fraud will not go unpunished. To such mechanisms prevention

methods of detention must be added, they can indeed be identified symptomatic signals of an illegal activity in progress, of a *misappropriation* which has already been consumed or is about to be consumed: a) accounting anomalies; b) procedures and reports as unrealistic as they could be too large money transactions or business meetings in unusual places and times; c) sudden improvement in lifestyle of some employee; d) suspicious behavior in general. To these *red flags* if they do could add others, they are only clues, to date the technological equipment and IT in companies is an equally efficient deterrent.

Finally, a very important role in the *misappropriation* of corporate assets is also carried out by government authorities which should be equipped with specific tools to combat these crimes, in fact, often the law enforcement officers charged with investigating them subjects lack the knowledge necessary to investigate within the complicated business complex that is its primary habitat.

**3.6 The misrepresentation**

According to the definition provided by the "Association of Certified Fraud Examiners", the*misrepresentation,* (also *financial statment fraud* ) is "the voluntary practice of representing in the balance sheet a fallacious patrimonial situation so as to conceal the real conditions financial statements to users of the financial statements ". Again fraud in examination is mainly performed by the *upper management* of the companies for reasons that can be traced both in

their remuneration systems and in the greater ease of access to the company's accounting area. The phenomenon of *misrepresentation* is also it much more widespread than one might think, has been observed (Harris and Bromelis, 2007), analysing a sample of 845 listed companies, which one in 10 companies are victims of such fraud, in reality this data translates into a probability of 8.77% that the company carry-overs of forgeries in the financial statements. Like the *misappropriation* of *assets* also the *misrepresentation* causes serious damage, not only in the societies in which it is perpetrated, it has indeed negative externalities that also affect other *stakeholders*.

The weight of the *misrepresentation* in corporate losses can be seen from the graph below due to fraud.

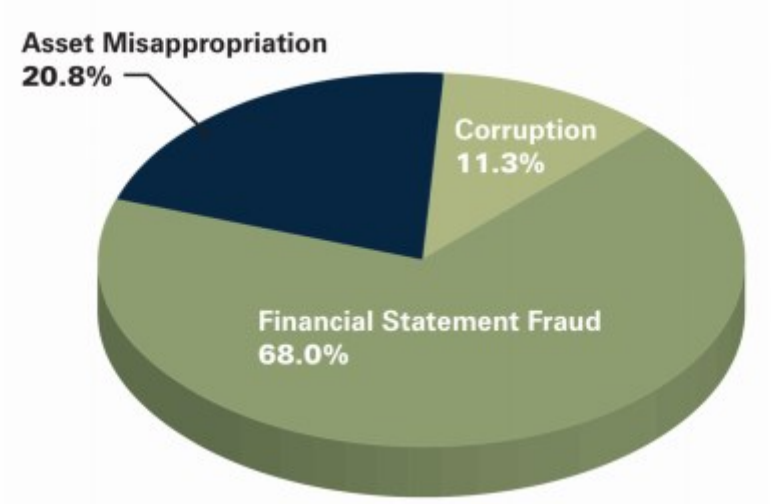


*Figure 2.3 - Percentage of total losses reported (Source: ACFE, 2010)*

The *misrepresentation* can then be categorized into different types, first of all it must distinguish between the financial (which will be widely discussed) and the non-financial one, the financial one foresees the underestimation of the company activities or the overestimation; in the case of financial *misrepresention* of the second type therefore distinguishes between: a) forgery of revenues; b) concealment of liabilities / assets; c) false disclosure; d) false valuations in

on the value of assets and / or liabilities. The non-financial *misrepresentation* has ad subject: a) falsification of employee credentials; b) manipulation of documents interior; c) manipulation of external documents (fig. 2.4).

The main causes of fraudulent financial statements have been shown to be:

a) compensation incentives for managers

b) a lower performance than the industry average or those of the past.

In the second case, the aim of falsification in the financial statements lies in the desire to conceal a

worsening of the real performance in order not to bring down the price of the stock, in general the more the companies deviate, negatively, from the average trends of the sector plus these


*Figure 2.4 Classification of the various types of misrepresentation (Source: ACFE, 2010.)*

they have an incentive to falsify the operating results. This motivation is linked to before; in fact managers are often paid with a variable system that provides incentives the higher the better the results achieved. In particular, when the managers' remuneration is carried out through *stock options,* the incentive to falsify the balance sheet is even greater, this is because this compensation system is not linear, managers they are all the more likely to exercise their pre-emption rights on company shares the higher the price of the underlying, that is, of the

shares themselves and therefore also the value of the *calls* in their possession, therefore they have a great interest in the growth of the price of securities market and to achieve this goal may feel justified for example to omit losses or to falsify operating results in the financial statements. From an investigation conducted by the GAO (General Accounting Office) on the financial statements of 845 US companies between 1997 and 2002, it emerged that there were 919 budget reclassifications during this period of which 100% proved to reflect an underlying fraudulent activity. Also for the *misrepresentation* of the financial statements ACFE has identified *red flags* : a) an increase in the financial leverage (third party capital / own capital); b) transactions involving large amounts and unusual at the end of the business year; c) large risky investments; d) distribution managerial incentives for unjustified growth prospects; e) lack of controls internal or adequate surveillance systems.

Furthermore, as for the *misappropriation* of *assets,* also for *misrepresentation it* is possible implement an effective preventive and custodial system that includes: a) an analysis vertical; b) a horizontal analysis c) an analysis of the various company indices. Vertical analysis relates the value of each balance sheet item to the overall value in its category (the sum of each ratio must be equal to 1). With analysis horizontal, on the other hand, the value of each balance sheet item is compared year by year and evaluated any increase or reduction thereof.

The index analysis deals with reporting various balance sheet items, such ratios can be compared with those of other companies in the sector ( *cross-section* ), or with those of the company itself of previous years. As for the *misappropriation* of *assets* company also to prevent *misrepresentation* measures must be taken internal security very similar to those already mentioned in the previous paragraph.

### 3.7 Famous cases of financial fraud

The history of financial crimes is full of cases that ended with the conviction of the various creators,

who with their scam schemes have defrauded thousands of people and sometimes whole organizations. Tom Petters[33] was a Minnesota businessman, managing director of the company by him founded, the Petters Group Worldwide. In 2005 he was sentenced to 50 years in prison for setting up a $ 3.65 billion Ponzi scheme, the largest in history afterwards that of Bernard Madoff and Allen Stanford. Petters and his associates convinced him investors to hand over their money to buy electronic equipment that they would have been resold to companies like Costco and Samsclub, in reality these purchases did not were carried out and the money was used for personal purposes by Petters himself. The scam it was discovered when in 2005 the company's vice president testified that

[33] Jon Schiller,2010: Financial Fraud (Pag.51)

he had collaborated in the realization of the scheme. Allen Stanford[34] was the Texan financier who was investigated in February 2009 by Security Exchange Commission for devising a $ 7 billion Ponzi scheme. The Stanford family built his fortune thanks to the growth of the real estate market in the United States 90s of the last century. Together with his father he founded the Stanford Financial Group which it allowed Stanford to build a great scam system. Of unsuspecting investors

they were persuaded by the bank 's brokers to sign fake bank certificates of deposit Stanford Bank, which apparently offered 3% higher yields than certificates of deposit from other US banks. This alleged change was related to the fact that the certificates were issued by an offshore bank on the island of Antigua, including Stanford he was the owner. With the 2008 crisis, however, Stanford Bank suffered serious losses investors began to ask for their savings back and numerous checks came carried out by the SEC and the FBI[35] who discovered the existence of a large Ponzi scheme at the basis of the flow of money that came to the Stanford bank. He was arrested in June in 2009 and 2012 he was sentenced to serve a 110-year sentence in a federal prison of maximum security in Florida. The most emblematic case in the context of financial *misrepresentation* was that of a

[34] Consulted on 25.11.2019: https://www.nytimes.com/topic/person/robert-allen-stanford
[35] Definition: **The FBI** is a government agency in the United States that investigates crimes in which a national law is broken or in which the country's security is threatened. **FBI** is an abbreviation for 'Federal Bureau of Investigation'.

that Martin Armstrong[36] who in the late 1990s was accused of hiding his losses of its investment fund by falsifying its real Net Asset Value[37]. Between 1992 and 1999 Armstrong issued bonds of his company for a total value of $ 3 billion in favor of 139 Japanese institutional investors guaranteeing them yield of 4% and that the proceeds would have been invested in US government bonds;

Armstrong hid losses from various investments until 1999, upon reporting of a Japanese investor, the SEC opened an investigation against the financier who came accused of making false statements about the real value of his fund and punished with 7 years in prison.

Another famous fraud case was that of trader Nick Leeson[38] who came in 1995 sentenced to six and a half years in prison for causing the bankruptcy of Barings Bank[39]. He with his speculative activities led the bank to financial collapse. Although at the beginning of its activities the lack of scruples in trading allowed Barings Bank of earn big profits, in a few years this proved fatal. Leeson,

---

[36] Consulted on 28.10.2019: https://www.newyorker.com/magazine/2009/10/12/the-secret-cycle

[37] Definition Investopedia: The net asset value (NAV) represents the net value of an entity and is calculated as the total value of the entity's assets minus the total value of its liabilities

[38] Consulted on 14.09.2019: https://www.next-finance.net/How-Nick-Leeson-caused-the

[39] Definition Business Dictionary: A British merchant bank, established in 1762 and for many years considered the most stable bank in the world. The bank collapsed in 1995 as a result of unauthorized speculative trading by an employee named Nick Leeson. The bank was taken over by ING.

Read more: http://www.businessdictionary.com/definition/Barings-Bank.html

passed by Morgan Stanley[40] at Barings in 1989 made a rapid career and was appointed manager for *futures* transactions on the Japanese market. In 1992 he began to carry out operations unauthorized that soon led to the accumulation of increasing losses, much that these went from $ 2 million to $ 208 million in two years. Leeson however tried to hide these losses in an account he created, account 88888. May 16, 1995 Leeson opened a short position for $ 8 billion in *straddle* 1 on the Japanese index for one The *straddle* is a strategy performed with options to speculate or to hedge on the performance of the underlying. It consists in the simultaneous purchase of a *put* and a *call* in order to be covered by both rises both from any falls in the underlying. In fact, if the value of the action or as in this case of a index will go up the *call* can be exercised , if it goes down the *put* will be exercised . Whoever sells a *straddle* , as in case of Leeson, is convinced that the market will remain static, at least for a certain period of time, and that it can huge amount of money, convinced that the Asian market would remain stable in them very short term. However, the following day there was a catastrophic earthquake in Kobe which caused the Nikkei index[41] to collapse causing serious losses to Barings, who they came to about $ 1 billion. In February

[40] Business Dictionary definition: International financial firm, which specializes in providing investment and other services to individuals and businesses

Read more: http://www.businessdictionary.com/definition/Morgan-Stanley.html

[41] Definition Investopedia: The Nikkei Index, also commonly referred to as the Nikkei 225, is the most recognized Japanese stock market index.

1995 Leeson fled to Singapore where he came arrested on March 2 of the same year. Barings Bank went bankrupt and was purchased from the Dutch ING[42] for the symbolic amount of $ 1.

The history of these scammers is often very similar, usually people extremely ambitious, confident of themselves and of impunity, driven by the desire to get rich, ready for anything for their purposes. Temporarily, their events intertwine in the years of economic boom in the United States, when people, as well as financial institutions and large corporations began to convince themselves that this huge growth could not be achieved stop. As can be seen from the dates, each of them started his fraudulent activity in a particularly prosperous period for the economy to then be discovered and condemned in correspondence with the explosion of the speculative bubble that had gone to inflate afrom the mid-80s.

*" It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so "* (" It is not what you do not know that you get into trouble, it is what you give for sure that instead it is not "- Mark Twain, 1835-1910).

### 3.8 The Bernard Madoff case

The largest Ponzi scheme in history Bernard Madoff's story is not unlike that of the other scammers that have been mentioned, he was a brilliant businessman

[42] Definition investopedia: A Dutch investment Bank

before he started his business fraudulent in the 90s, he held important positions such as that of President of the NASDAQ, the list of American technology titles. The real peculiarity of the story is the extent of the fraud conceived and committed: a $ 65 billion Ponzi scheme that caused it the sentence of 150 years in prison. Of Jewish origins, at the age of 22, Madoff started his first business in a company of investments. Over the years he gained more and more experience showing a great talent for business and was one of the first to adopt new computer trading technologies[43]. In the 1990s he was the sixth market maker with his company, Madoff Investment Securities collect a double prize from the simultaneous sale of two options that will expire without being exercised, if the forecast is incorrect, the losses can be very large. on Wall Street[44]. It was precisely through this company that Madoff during the 90s and in the early 2000s he managed to get huge assets not only from simple investors,

but also by the largest financial institutions in the world, so much so that banks like Unicredit, HSBC, the Spanish Bbva, BNP Paribas and Union Bancaire Privèe were found exposed with fraud in the amount of $ 75 million, $ 1 billion

[43] Lionel S. Louis, 2012: Bernard Madoff and His victims
[44] Definition Colin's Dictionary: **Wall Street** is a street in New York where the Stock Exchange and important banks are. **Wall Street** is often used to refer to the financial business carried out there and to the people who work there.

respectively, $ 300 million, $ 850 million and $ 470 million. It is legitimate to ask how it is possible that for about twenty years he managed to defraud investors with different skills and knowledge. Madoff made a complicated and intricate Ponzi scheme, as it guaranteed constant returns of 10% per year, regardless market trends. Investors saw Bernard Madoff as a man extremely serious and reassuring, no one would have doubted the legality of his actions. The SEC inspected its offices in 2004, 2005 and 2006 without finding any trace of illegality, in fact Madoff had been very skilled in creating, through the falsification of accounting records, of investment activities never performed.

The strategy that Madoff claimed to implement to obtain these returns was the *split-strike convertion*[45] , the steps of which envisage: a) the purchase of shares representing a index like the S&P 500; b) the sale of *call options out of the money* , that is, with a price higher than the current price; c) the purchase of *put options* with a price of year very close to the current price using the premium received for *calls.* By bragging about this strategy, Madoff justified higher returns compared to other risk-neutral hedge funds. However, a careful study of the Sector returns would provide Madoff investors with evidence that something

[45] Definition from seeking alpha: The split strike strategy involves buying a basket of stocks, then writing call options against those stocks, and finally using the proceeds from writing the call option to purchase a put option.

opaque was hidden behind its performances. In fact, the Madoff bottom and the attached *feeders funds* were not the only ones on Wall Street to invest through the *split strike convertion* , but they were the only ones who, at the same risk, obtained such high returns that they wandered between 10% and 12%. The graph in Figure 2.5 represents the returns of the Madoff funds and the EMN fund that followed the same strategy and was equally risk neutral, each However, the returns of this year were lower than those of the other funds. We can therefore infer that overall such high returns should have triggered a

alarm bell, this could then also be confirmed by other "red signals" for investors: *alphas* too high compared to the average, volatility too low, extreme

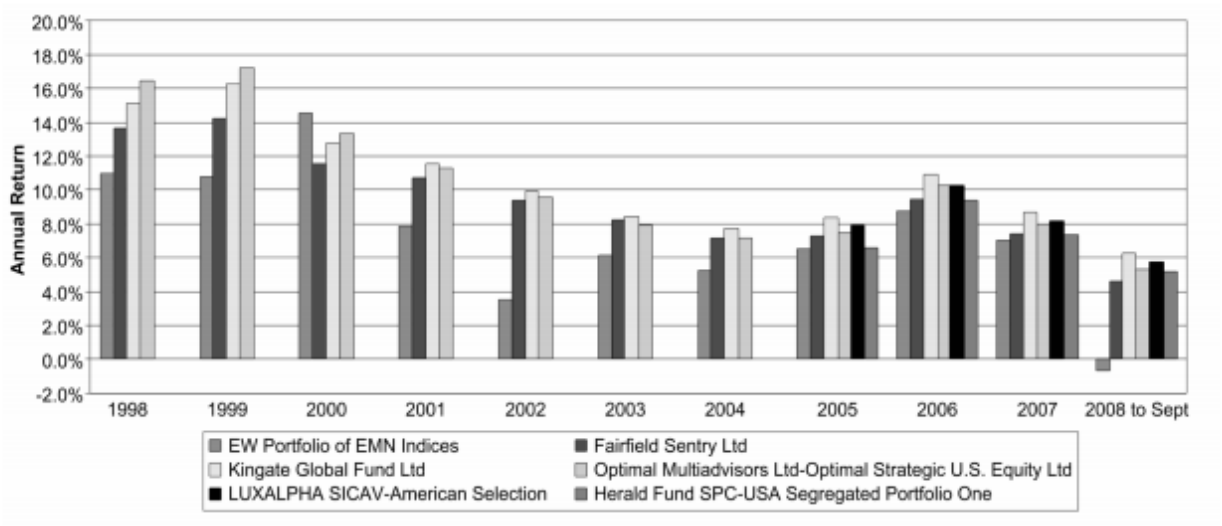



*Figure 2.5 - Returns of Madoff's feeder funds and the EMN Index Portfolio (Source:Thomas Schneeweis and Edward Szado, 2010.)*

difficulty accessing information regarding *asset allocation* policies.

When Bernard Madoff handed over to the authorities on December 11, 2008, his story had a huge media impact, much more than the stories of other scammers who already are been mentioned. This is because the consistency of the economic damage it caused is directly indirectly, it involved a very large number of investors, unaware of the big one fraudulent mechanism. Madoff has always said that he never realized the seriousness of his actions claiming that the fraud implemented had the characteristic of temporariness.

In the world of investments, the continuous and obsessive pursuit of high performanceit deters investors from maintaining adherence to reality. " *When one thing is too much beautiful to be true is because it is not true* "(From Quentin Tarantino's film" Inglorious Basterds",2009).

**3.9 The Evolution of the phenomena**

In order to go into detail on the case that we are going to analyse, it is necessary to name some types of computer fraud that have arisen in recent years which have the ultimate purpose of defrauding investors and shareholders. The advent of technology has improved the lives of the world's population in many ways thanks to the speed with which it is possible to exchange information and make economic transactions. At the same time, however, the speed at which these new technologies travel makes the work of surveillance agencies to protect consumers

increasingly difficult, as they must continually develop new ways to combat fraud, but also develop techniques to anticipate fraud.

The United States is, today as in the past, a country strongly affected by fraud computer. In the United States, cyber fraud is believed to complement fraud details of federal wire fraud and mail fraud offenses. Precisely, the crime of "Wire fraud" occurs when "someone has appealed or has intended to appeal to any means or device to defraud or to obtain money or other utilities a

by means of false or misleading pretexts and transmits or causes it to be transmitted by telegraph any written, signature, sign, drawing or acoustic signal to the purpose of realizing such means or artifice ": here fraud for telecommunications medium. Instead, there is a crime of "mail fraud" when using it the postal service between different states or with foreign countries to plan or execute a fraud. The broad formulation of the two criminal hypotheses and, in particular, the failure provision of the deception of a person as an extreme necessary constitutive of the crime, has easily allowed the doctrine to fit into these hypotheses the new figures of telematic fraud. In particular, the US doctrine has considering the equivalent electronic connections, for the purposes of configuring the offenses in question, to telegraphic communications. Given the expansion of the phenomenon, in the middle of the eighties, the Counterfeit Access Device and Computer were issued Fraud and Abuse Act regarding abusive access to IT

systems, and Credit Card Fraud Act to specifically crack down on card fraud credit.

With the first provision, an unauthorized access figure was provided for a Qualified "Federal interest computer" with the intent to commit a fraud (18 U. S. C. § 1030 (a) (4)) (computer access fraud): a provision which, although opposed during the preparatory work of the law, considering the requirement of abusive access to the system to be unnecessary and misleading computer scientist used to use the fraud, remained almost unchanged even after the numerous legislative interventions that affected § 1030 U. S. C. during this years; the only changes made with the most recent “National Information Infrastructure Protection Act "of 1996, on the other hand, if on the one hand they rather aim at a narrowing of the scope of operation of the standard, through the exclusion of cases of mere improper use of the computer, which entailed a cost total not exceeding $ 5,000 over a year; on the other side, by replacing the term "computer systems of federal interest" with the broader "protected computer system", intended to operate for all the provisions of § 1030, are limited to expanding the scope of computer systems whose fraudulent use determines criminal relevance at the level federal conduct of the offender.

The second rule, however, provides various criminal hypotheses: a) when it is produced, yes you use or transfer one or more counterfeit access tools; b) when

used one or more unauthorized access tools during the one year period and through such conduct will provide you with an unfair profit of $ 1000 or more for the period in question; c) when you have 15 or more counterfeit or non-counterfeit instruments authorized; d) when you own, own or trade with equipment for create access tools. All these crimes presuppose an element subjective constituted not only by the conscience and the will of the conduct, but also by awareness of the nature of the tools used or held with the specific intent to defraud. The first hypothesis is punished with a non-pecuniary penalty greater than $ 50,000 or double the value obtained with the crime and / or with a penalty prison of no more than 15 years; if the offense was committed after the imprisonment for another offense of the same type, or after an attempt to commit an offense of the same type, the sanction consists of a pecuniary penalty not exceeding $ 100,000 or double the value obtained with the crime and / or with the prison sentence not exceeding 20 years. The second and third hypotheses are considered less serious and punished with a lesser penalty; the fourth hypothesis, however, is punished as the first, but not the punishment for reoffending is expected to increase. It is sanctions that constitute a significant increase in the penalties provided for in the "Truth in Lending Act" and in the "Electronic Fund Transfer Act" and yet very elastic, so as to allow the judge a high margin of discretion regarding the measure concrete penalty and the possibility of applying the monetary penalty only without a minimum edict. The standard also dictates a series of definitions of terms used

in law itself. In particular, it defines the notion of access tool as "any card, nameplate, code, account number or other means of accessing the account that they can be used, alone or together with other access tools, to obtain money, goods, services or anything else of value that can be used to activate

an electronic transfer of funds, excluding those originating only from one paper tool ".

The expression "other means of accessing the account" is also of very broad meaning and includes, for example, the personal identification number, the so-called P.I.N. is the other biometric means of identification of the person. The expression "tool of counterfeit access ”includes any access tool that is counterfeit, fictitious, altered or falsified or an identifiable component of an instrument access or a counterfeit access tool. By "component" we mean, however, incomplete access tools such as blank credit cards, microchips, signatures, holograms and magnetic strips.

Unauthorized access tool is any lost, stolen, revoked or canceled, or that was obtained with the intention of defrauding. Finally, "producing" means drawing, altering, authenticating, duplicating or assembling; "Transfer" means, instead, sell, rent, lend, distribute, purchase, obtain possession or detention. The standard also establishes an Office of the Secret Service of the United States to ascertain the crimes foreseen by the law according to the modalities established between the

Secretary of the Treasury and the General Attorney. At the state level, on the other hand, it is also controversial in the United States whether the rules apply computer fraud scam despite the lack of a deceptive person.

Doctrine controversies have led some states to enact laws with which the rules regarding fraud against IT fraud are extended; other states, instead, they preferred to enact provisions that provide for computer fraud such as autonomous crime figure.

# IV CHAPTER

## 4.The Fyre Festival Case

### 4.1 Billy McFarland

Billy Mcfarland was born on December 11th 1991, in New York from a humble family whose parents were two real estate developers. Billy showed to be different from his peers since his early ages in fact, his “entrepreneurial spirt” kicked at  a very young age.  Since he was in fifth grade in middle school he allegedly found a way of hacking the school’s computer system in order to promote his own web-posting business.  Was when he was 13 years old that he founded his first company, an online outsourcing business that coordinated clients with designers. After graduating at Pringry High school he attended the Buckenell University in a computer engineering course even he dropped the college at the

end of his freshmen year. That's when his started his career as an entrepreneur. Billy's Fyre Festival scam was surely not his first, since it's reported that his first major scam happened in 2013, when after launching "Magnises" a black card targeted to millennials that was compared to the American Express black card. These two cards had some similarities such as, they were both black, made of metal and promised exclusive perks to members. For a $250 annual fee, Magnises members could experience the rush of paying checks with a heavy card. But more than that, Magnises billed itself as a social club for millennials, connecting their members through exclusive events and offering tantalizing deals to the aspiring American Express black card set. As per Magnises' Facebook page, "Our members are the thrill-seekers, the hard-workers, & the go-getters. We are an international group of people looking to create and maximize our experiences."

However, it was later discovered that the Magnises card wasn't an actual card but it only copied the magstripe information from a costumer existing card. By the end of 2013 the Magnises club had more than 500 members and amassed more than $1.3 million. It started to fall apart as soon as clients started to complain that the service was not what it promised to be, and as we will state later on the thesis is a pattern that Billy used in his modus operandi. It was only after the Fyre Festival that Magnises would declare bankrupt. The Magnises card allowed Billy

to gain credibility as an entrepreneur around New York and prepared him for the Fyre Festival.

### 4.2 The Fyre Media and the Fyre Festival Fraud

In the beginning of 2016, Mcfarland founded Fyre Media app, an online platform with had the aim of connecting consumers and celebrities, by allowing its members to book famous people for their private events by making an offer on the app. Later that year in order to promote the Fyre Media app, Mcfarland founded the Fyre Festival, a new concept of music festival that was supposed to be held in the Bahamas in two weekends of April and May 2017. The festival was suppose to offer to the consumers a one in a life time luxury experience, it offered in fact a package that included private jets to get to the Bahamas, extravagant villas and gourmet food and VIP yatch experiences with celebrities.

In order to convince investors to invest in the Fyre Festival he promised via non registered investment contracts rights to investors in the festival's commercial enterprises. Between 2016 and 2017, Mcfarland raised approximately $ 7.9 million from at least 43 investors in the Fyre Media offerings and $ 16,5 million from at least 59 investors on the Fyre Festival offerings. In providing investors with the requested documents Mcfarland:

- Made false allegations regarding Fyre Media and Fyre Festival financial metrics and assets such as: sending per email false declarations on the

actual success of the Fyre Media app and the number of booked talents and creating false reports and spreadsheets exaggerating the company's overall success in order to convince investors to give him money. He was claiming to have thousands of offers who represented millions of dollars in performances, when in reality only 60 bookings were made and the revenue was of only $57.443.

- False Statements Concerning a Fake Brokerage Statement, McFarland's Net Worth, Loans, and Investments: Under the request of investors he created a fake brokerage statement which showed that the owned &2.56 million in Facebook shares when in reality he only had $1.499 a very tiny fraction compared to the one declared in the email and texts sent to the potential investors. In one of his attempts to convince the banks to loan him money he made false declarations about his net worth and the company's revenue, and even if the loans were denied he told and provided documents to the investors claiming that the money was given and that it would serve as guarantee for their investments.
- False Statements Concerning Insurance and Agreements with Talent: as per induce investors to invest Mcfarland falsely told them that they would have full insurance coverage in case of event cancelation as such policies in reality were never executed, when the event was cancelled the investors lost their investments in full.

- McFarland and Fyre Media Engaged in a Scheme to Create the Illusion that Magnises was the Subject of an Imminent Acquisition: numerous false statements and documents were created in order to give investors the illusion that Magnises was about to be purchased by a third party for an amount of money between $ 35 and 40 million. The whole scheme had the solely aim of creating a false impression that Mcfarland was a successful interpreneur with a proven track record of success.

### 4.3 The SEC vs Billy Mcfarland

This section of the thesis will analyse the lawsuit that the Security and Exchange commission filled against Billy Mcfarland and Fyre Media, contesting the fraudulent activities aforehand mentioned and the consequent consequences.

The Security and Exchange Commission, an independent federal government agency responsible for protecting investors[46], decided to fill a complaint against Mcfarland and his enterprises, claiming the violation of the antifraud provisions of the security laws as the following:

- Using instrumentalities of interstate commerce or emails to create

[46] Reference: https://www.sec.gov/

false material that would be operated to fraud and deceit investors (section 10(b) of the exchange act).[47]

- Engaged untrue transactions to obtain money or/and property for misleading and fraud purposes ( section 17a (1) (2) and (3) of the securities act)
- No registration statement was made with the Commission as the law requires about transactions, the contracts or the documents involved in Fyre Media. Unregistered securities were sold or offered in interstate commerce( section 15 (a) and (c) of the securities act).
- Mail use was made to effect transictions in attempt to induce the purchase of share of stocks and convertible promissory notes in Fyre Media (section 15 (a) of the exchange act).

For the aforementioned reasons Mcfarland and the Fyre Media enterprise were put under accusation with two counts of Wire fraud and in March 2018, Mcfarland pleaded guilty for both counts and admitted to using false documents to attract investors to put more than $26 million into his company. The SEC won his battle against Billy Mcfarland and he was sentenced to six years of conviction in a federal prison.

[47] Consulted on 04.06.2019: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-141.pdf

The media impact that the Fyre scandal had plus the tempested intervention of the SEC the case was solved and the damage partially covered. But, what if the Fyre festival was organized on blockchain? Is this technology able to help companies prevent financial frauds?

## 4.4 Use of Blockchain to prevent Financial Frauds

There are many reasons why using the blockchain technology might help in the prevention of financial frauds, one of them is related to how complicated financial transactions are, for example, the needed time for settlements, a third-part mediation or the fact that multi-step processes often require a human interaction. This reasons can make financial transactions an easy target for fraudsters but the implementation of the blockchain technology can reduce the percentage of frauds as the information contained in the transactions would be shared in real time so that time, costs and opportunities to commit fraud would be drastically reduced.

### 4.4.1 Digital Identity Fraud

According to IBM[48] researchers, in 2018 only, identity frauds costed consumers $16 billion, and only the 16% of companies said they could detect fraudulent attempts. Living in an era where all of our personal data is shared and exposed on

[48] Consulted on13.12.2019: https://www.ibm.com/security/fraud-protection

a daily basis on websites and social media its very easy to be a target of fraudsters when stored in centralized databases. For this reason, it would be useful to use a technology who would allow our personal data to be protected in a way in which we would be secure to share them. The distributed ledger feature of the blockchain technology would help in the prevention of identity frauds and grant consumers more ownership on their on data. An example of identity fraud that can be avoided with the blockchain technology is the "New account application fraud[49]": a fraud that happens when fraudsters take real personal information and mix it with fictional one, in order to fabricate an entirely new account. This new account could be used to fraud banks by opening and using checking accounts, duplicate credit cards and get access to financial information. By creating a digital mechanism that verifies identities at the exact time of any type of transaction, security would move from data aggregators to the root owner, and that's what blockchain would do. A self-sovereign[50] solution where both individuals and companies would compile a lifetime's worth of identity data while maintaining control and taking part of different transactions. By doing so, identity frauds would be extremely unlikely to succeed and there wouldn't be need for companies to store personal data. A recent example is represented by the Facebook Security Scam The Facebook Security Scam is an instance of social media fraud, which was specially designed to separate social media users from

[49] Consulted on 18.12.2019: https://www.experian.com/decision-analytics/account-openinfraud
[50] Consulted on 18.12.2019: https://www.nasdaq.com/articles/how-blockchain-can-fight-fraud-based-know-your-customer-data-2019-02-11

their money. In the year 2012, scam pertaining to Facebook was developed in an attempt to steal financial information from their users. Hackers hijacked the user accounts by impersonating the security set up by Facebook. These hacked accounts were used to send fake messages to other users by warning them that their account was about to get deactivated and thereby, instructing the users to click on a link to verify their account. Post this, the users were directed to a false Facebook page which asked them about their account credentials as well as the credit card information in order to secure their account.

### 4.4.2 Supply Chain Fraud

A supply chain can be defined as a network of individuals, organizations, activities, resources and technology involved in the creation and sale of a product[51]. A supply chain management involves the oversight of the information, materials and finances of the network so it can be stated that it's a complex process that involves different parts, and for this reason can be an easy target for frauds.

According to the Financial Cost report of 2019, fraud costed businesses and individuals around the world an amount around $ trillion every year.

The usage of the blockchain technology may help prevent it with:

[51] Consulted on 13.12.2019: https://www.investopedia.com/terms/s/supplychain.asp

- Traceability who would improve the operational efficiency by mapping and visualizing enterprise supply chain, allowing companies to understand their supply chain and provide consumers with real and immutable data.
- Transparency: the information contained in the ecosystem would be updated in real life and the processes would be open and available to all the stakeholders.

In the specific case of the Fyre Festival, if the event was built on blockchain the function of smart contracts would have helped all he parts involved. The project could have been designed with milestones that that would allow investors to release their capital commitments once the conditions were met, in this way the investors would be able to control the progress made on the project and in case some documents were modified, the immutability condition of the blockchain would allow investors to have access to the original document and decide whether to continue to invest or to bounce out of the investment and take their money back. In the case of the attendees the smart contract could have been made in such a way to allow the clients to demand status updates on all the services that were promised at the moment of the contract stipulation for example the luxury villas, the performers, the food etc, so the whole process would be

transparent and the clients would exactly know what to expect from the organizers.

## Conclusions

In developing this thesis, a basic insight into the functioning of blockchain technology was provided. It was subsequently discussed how the use of this same technology can benefit the area of corporate governance, which can greatly benefit from such use. The role of frauds in financial history, past and modern, was discussed, and its consequent evolution with the advent of technology. Finally, a recent case of financial fraud, the Fyre Festival Case and its outcomes, was considered. Finally, some suggestions are given on how to use this technology, cases such as the aforementioned can be prevented.

It can therefore be said that blockchain technology can, if properly developed and used, make transactions, not only of individuals but also of companies, simpler and safer and guarantee a reduction in the risks of fraud to which we are exposed every day. The purpose of this thesis is to act as a suggestion for companies and individuals to consider blockchain technology at the moment as the most complete solution to problems related to scams.

# Bibliography


Tim Mathis,2016 Ebook: A Guideline to Blockchain, the technology behind bitcoin

Sally Ramage,2006: A Comparative Analysis of Corporate Fraud

Imrar Bashir, 2018: Mastering Blockchain

Alan T. Norman, Everything about the Blockchain technology

Mauro Bellini, 2018 : Blockchain and Bitcoin

Umit Hacioglu, Ebook: Digital Business strategies in Blockchains ecosystems (pag.68)

David Lee Kuoo,2018: Handbook on Blockchain, Digital Finance and inclusion (pag.307) [1]

Srinivas Mahankali, 2019: Blockchain the Untold story

Melanie Swan, 2015:Blockchain a Blueprint for new Economy

Larry A. DiMatteo, 2019: The Cambridge Handbook of Smart contracts

Vincent Hale,2018: Launch an Ico and Token Crowsdale

Shatoshi Nakamoto,2019: The white Paper

Edward J. Balleisen, 2018: Fraud: An American History from Barnum to Madoff

Kerry Gan,2019: Unlock the Secret of Ethereum

Umit Hacioglu, 2019: Blockchain Economic and Financial Market Innovation

Sympiossium Proceedings: 2018 (pag.482)

Rodrigo da Rosa Righi, 2019: Blockchain Technology for industry 4.0

IMinds,2014: Ponzi Schemes

Irene Finel- Honignam, 2009: A Cultural History of Finance

Books Llc,2010: Ponzi and Pyramid Schems

Harold Kent Baker, Greg Filbeck,2017: Hedge Funds: Structure, strategies and performances

Lionel S. Louis, 2012: Bernard Madoff and His victims

Albrecht, C., Kranacher, M. J., & Albrecht, S. (2008). Asset misappropriation research white paper for the Institute for Fraud Prevention. Institute for Fraud Prevention, Research studies, Working paper.

Bollen, N. P., & Pool, V. K. (2012). Suspicious patterns in hedge fund returns and the risk of fraud. The Review of Financial Studies, 25(9), 2673-2702.

Cicero, M. T. (1961). De Officiis. Translated by Walter Miller.

Lo, A. W. (2015). The Gordon Gekko effect: The role of culture in the financial industry (No. w21267). National Bureau of Economic Research, 1-44.

Nebbia, G. (2007). Piccola Storia delle Frodi (No.12). Altro Novecento.

BELLINI M. (2017). Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia.

## Sitography


https://www.economist.com

https://bitcoin.org/bitcoin.pdf

https://www.europarl.europa.eu

https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf

https://www.experian.com/decision-analytics

https://www.nasdaq.com/articles

https://www.investopedia.com

http://www.businessdictionary.com/

https://www.mycryptopedia.com

https://www.gsb.stanford.edu

https://medium.com/

Misappropriation of Assets: A Test of SAS No. 82 Risk Factors

books.google.it › books

https://www.nytimes.com

https://www.next-finance.net

https://www.equities.com/

https://www.sec.gov

https://corporatefinanceinstitute.com/

https://capital.com/it

https://www.investorlawyers.com

https://www.standard.co.uk/ -

https://www.crowdfundinsider.com

https://www.nysscpa.org

https://completemusicupdate.com

http://gossiptoday.altervista.org/

https://www.dailymail.co.uk/

https://www.spin.com

https://www.ibm.com/blockchain