**BLOCKCHAINS TECHNOLOGY: FIRST PART.**

 **INTRODUCTION, PRELIMINARY INFORMATION AND THE HISTORY OF THE BITCOIN**

**I LESSON:**

**INTRODUCTION OF BLOCKCHAIN TECHNOLOGY AND A BRIEF HISTORY OF THE BITCOIN**

, In the first part I will focus my attention on the blockchain technology and on its first product: the cryptocurrency known as bitcoin. In the second part I will speak about the applications (also the potential ones) and about the bitcoin sons, i.e. the altcoins. More in detail in these first 10 hours, I will speak about the history of the bitcoin and the taxonomy of the products of this new technology. The technology is developing in a tumultuous way. Few year ago, there was only Blockchain 1.0, the Internet of money. After few year it was developed Blockchain 2.0, the internet of business and now we are in the age of Blockchain 3.0, the internet of everything. I will describe the problems connected with illegal markets that arise from the anonymity of this currency. I’ll spend few words how Bitcoin and the other cryptocurrencies were used as modern “smart” Ponzi’s scheme to fraud people. Then I’ll consider more technical questions describing the strategy used by Satoshi Nakamoto, the creator of the bitcoin, to solve the consensus problem. I will speak about Byzantine Generals’ Problem and I’ll will consider also the problem to reach a consensus through an election ( the Arrow, Borda and Condorcet contributions will be described). The CAP Theorem will be briefly analysed and I will sketch the history of cryptography till the elliptic curves. I will speculate also about the future developments of the cryptography, i.e. the quantum computing. The strange phenomena that occur in quantum mechanics and their potential fall-out on the cryptocurrency world will be described. Lastly I will describe how the blockchain technology is applied in bitcoin. The ancestor of the bitcoins: the rai money of the Yap island, will be described. The way to avoid Sibyl attack will be illustrated in detail. I will speak about miners, the use of the bitcoins as the reward for the mining activity and the modern technologies applied in mining (GPU rig, ASIC, FPGA). I will quantify the great amount of energy necessary to produce new bitcoins. Finally I will answer to the million dollar question if Bitcoin is a “real” money and if its present value is fair. I will analyse also how is really anonymous the use of the bitcoins in the payments. Lastly I will speculate about the possible future of the cryptocurrencies.

**Bitcoin is a cryptocurrency and worldwide payment system. It is the first decentralized digital currency**, as the system works without a central bank or single administrator. The network is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes through the use of cryptography and recorded in a public distributed ledger called a blockchain. **Bitcoin was invented by an unknown person under the name Satoshi Nakamoto and released as open-source software in 2009**. Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services. As of February 2015, over 100,000 merchants and vendors accepted bitcoin as payment.

 Research produced by the University of Cambridge estimates that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin. The technology on which bitcoin is based is the blockchain technology. **The blockchain is a public ledger that records bitcoin transactions. It is implemented as a chain of blocks, each block containing a hash of the previous block up to the genesis block of the chain.** A novel solution accomplishes this without any trusted central authority: the maintenance of the blockchain is performed by a network of communicating nodes running bitcoin software.

 Transactions of the form payer X sends Y bitcoins to pay Z are broadcast to this network using readily available software applications. Network nodes can validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes. The blockchain is a distributed database: to achieve independent veriﬁcation of the chain of ownership of any and every bitcoin amount, each network node stores its own copy of the blockchain. **Approximately six times per hour, a new group of accepted transactions, a block, is created, added to the blockchain, and quickly published to all nodes.**

This allows bitcoin software to determine when a particular bitcoin amount has been spent, which is necessary in order to prevent double-spending in an environment without central oversight. Whereas a conventional ledger records the transfers of actual bills or promissory notes that exist apart from it, the blockchain is the only place that bitcoins can be said to exist in the form of unspent outputs of transactions. In the blockchain, bitcoins are registered to bitcoin addresses. **Creating a bitcoin address is nothing more than picking a random valid private key and computing the corresponding bitcoin address**. This computation can be done in a split second. But the reverse (computing the private key of a given bitcoin address) is mathematically unfeasible and so users can tell others and make public a bitcoin address without compromising its corresponding private key.

Moreover, the number of valid private keys is so vast that it is extremely unlikely someone will compute a key-pair that is already in use and has funds. The vast number of valid private keys makes it unfeasible that brute force could be used for that. To be able to spend the bitcoins, the owner must know the corresponding private key and digitally sign the transaction. **The network veriﬁes the signature using the public key. If the private key is lost, the bitcoin network will not recognize any other evidence of ownership; the coins are then unusable, and eﬀectively lost.** For example, in 2013 one user claimed to have lost 7,500 bitcoins, worth $7.5 million at the time, when he accidentally discarded a hard drive containing his private key.

**Taxonomy of the blockchain technology:**

From 2009 to now, the blockchain technology changed a lot.

***Evolution of the technology***:

**Blockchain 1.0: Internet of Money** – ad example Bitcoin, Corda, Ripple

**Blockchain 2.0: Internet for Business** - ad example Ether, Tron, HyperLedger

**Blockchain 3.0 : Internet of Everything, Internet of IOT** - ad example Neo, Iota,

Another different taxonomy concerns the ***public or private nature.***

**Public blockchain:** Bitcoin, Ripple, Ether, Tron

**Private** **blockchain:** Corda, Hyperledger

**Mixed blockchain:** Neo, Iota, Ether 2.0

Private and public blockchain share many common features: both are peer-to-peer networks, where each participant maintains a replica of a shared append-only ledger of digitally signed transactions. Both maintain the replicas in sync through a protocol referred to as consensus. Both provide certain guarantees on the immutability of the ledger, even when some participants are faulty or malicious. **The sole distinction between public and private blockchain is related to who is allowed to participate in the network, execute the consensus protocol and maintain the shared ledger.** A public blockchain network is completely open and anyone can join and participate in the network. The network typically has an incentivizing mechanism to encourage more participants to join the network. Bitcoin is one of the largest public blockchain networks in production today.

**One of the drawbacks of a public blockchain is the substantial amount of computational power that is necessary to maintain a distributed ledger at a large scale.** More speciﬁcally, to achieve consensus, each node in a network must solve a complex, resource-intensive cryptographic problem called a proof of work to ensure all are in sync**. Another disadvantage is the openness of public blockchain, which implies little to no privacy for transactions and only supports a weak notion of security**. Both of these are important considerations for enterprise use cases of blockchain.

A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules put in place by the network starter. Businesses who set up a private blockchain, will generally set up a permissioned network. This places restrictions on who is allowed to participate in the network, and only in certain transactions. Participants need to obtain an invitation or permission to join. **The access control mechanism could vary: existing participants could decide future entrants; a regulatory authority could issue licenses for participation; or a consortium could make the decisions instead.** Once an entity has joined the network, it will play a role in maintaining the blockchain in a decentralized manner.

**History**

On **18 August 2008**, the domain name ”**bitcoin.org**” was registered .In November that year, a link to a paper authored by **Satoshi Nakamoto** titled Bitcoin: A Peer-to-Peer Electronic Cash System was posted to a cryptography mailing list. Nakamoto implemented the bitcoin software as open source code and released it in January 2009 on SourceForge. **The identity of Nakamoto remains unknown.** In January 2009, the bitcoin network came into existence after Satoshi Nakamoto mined the ﬁrst ever block on the chain, known as the genesis block. Embedded in the coinbase of this block was the following text**: The Times 03/Jan/2009 Chancellor on brink of second bailout for banks**. This note has been interpreted as both a timestamp of the genesis date and a derisive comment on the instability caused by fractional-reserve banking.

The receiver of the ﬁrst bitcoin transaction was **cypherpunk** Hal Finney, who created the ﬁrst reusable proof-of-work system (RPOW) in 2004. Finney downloaded the bitcoin software the day it was released, and received 10 bitcoins from Nakamoto. Other early cypherpunk supporters were Wei Dai, creator of bitcoin predecessor b-money, and Nick Szabo, creator of bitcoin predecessor bit gold. In the early days, Nakamoto is estimated to have mined 1 million bitcoins. In 2010, Nakamoto handed the network alert key and control of the Bitcoin Core code repository over to Gavin Andresen, who later became lead developer at the Bitcoin Foundation. **Nakamoto subsequently disappeared from any involvement in bitcoin.**

Andresen stated he then sought to decentralize control, saying: ”**As soon as Satoshi stepped back and threw the project onto my shoulders, one of the ﬁrst things I did was try to decentralize that. So, if I get hit by a bus, it would be clear that the project would go on.**” This left opportunity for controversy to develop over the future development path of bitcoin. **Laszlo Hanyecz** ”laszlo” made **the ﬁrst documented purchase** of a good with bitcoin when he bought **two Domino’s pizzas from ”jercos” for 10,000 BTC**. On May 17, 2010, Laszlo posted a request to buy pizza with bitcoin. It was on May 22 that he reported successfully trading 10,000 BTC for two pizzas, with Jeremy Sturdivant (jercos) jercos ordering the pizza and receiving the coins**. To commemorate the transaction, May 22 is dubbed Bitcoin Pizza Day**. Pizza providers worldwide oﬀer discounts to bitcoin users to commemorate Laszlo’s purchase.

Over the history of Bitcoin there have been **several spins oﬀs** that have lived on as separate blockchains. These have come to be known as ”**altcoins**”, short for alternative coins, since Bitcoin was the ﬁrst blockchain and these are derivative of it. These spin oﬀs occur so that new ideas can be tested, when the scope of that idea is outside that of Bitcoin, or when the community is split about merging such changes. **The ﬁrst fork of Bitcoin was Namecoin**, with discussions taking place on the Bitcointalk forum in December 2010. Another **early spin oﬀ was Litecoin**, which began in October, 2011. Since then there have been numerous forks of Bitcoin.

**The use of bitcoin by criminals has attracted the attention of ﬁnancial regulators, legislative bodies, law enforcement, and the media.** The FBI prepared an intelligence assessment, the SEC has issued a pointed warning about investment schemes using virtual currencies, and the U.S. Senate held a hearing on virtual currencies in November 2013. Several news outlets have asserted that the popularity of bitcoins hinges on the ability to use them to purchase illegal goods. In 2014, researchers at the University of Kentucky found ”robust evidence that computer programming enthusiasts and illegal activity drive interest in bitcoin, and ﬁnd limited or no support for political and investment motives.

A CMU researcher estimated that in 2012**, from 4.5% to 9%** of all transactions on all exchanges in the world were for drug trades on a single **dark web drugs market, Silk Road.** **Child pornography, murder-for-hire services, and weapons** are also allegedly available on black market sites that sell in bitcoin. Due to the anonymous nature and the lack of central control on these markets, it is hard to know whether the services are real or just trying to take the bitcoins. Several deep web black markets have been shut by authorities. **In October 2013 Silk Road was shut down** by U.S. law enforcement leading to a short-term decrease in the value of bitcoin. In 2015, **the founder of the site was sentenced to life in prison**. Alternative sites were soon available, and in early 2014 the Australian Broadcasting Corporation reported that the closure of Silk Road had little impact on the number of Australians selling drugs online, which had actually increased.

In early 2014, Dutch authorities closed Utopia, an online illegal goods market, and seized 900 bitcoins. In late 2014, a joint police operation saw European and American authorities seize bitcoins and close 400 deep web sites including the illicit goods market Silk Road 2.0. Law enforcement activity has resulted in several convictions**. In December 2014, Charlie Shrem was sentenced to two years in prison for indirectly helping to send $1 million to the Silk Road drugs site, and in February 2015, its founder, Ross Ulbricht, was convicted on drugs charges and faces a life sentence. Some black market sites may seek to steal bitcoins from customers.** The bitcoin community branded one site, Sheep Marketplace, as a scam when it prevented withdrawals and shut down after an alleged bitcoins theft. In a separate case, escrow accounts with bitcoins belonging to patrons of a diﬀerent black market were hacked in early 2014.

According to the Internet Watch Foundation, a UK-based charity**, bitcoin is used to purchase child pornography, and almost 200 such websites accept it as payment**. Bitcoin isn’t the sole way to purchase child pornography online, as Troels Oertling, head of the cybercrime unit at Europol, states, ”Ukash and Paysafecard have [also] been used to pay for such material.” However, the Internet Watch Foundation lists around 30 sites that exclusively accept bitcoins. Some of these sites have shut down, such as a deep web crowdfunding website that aimed to fund the creation of new child porn. Furthermore, hyperlinks to child porn websites have been added to the blockchain as arbitrary data can be included when a transaction is made.

**II LESSON**

**BITCOINS AS PONZI SCHEME. THE CONSENSUS PROBLEM.**

**Bitcoins may not be ideal for money laundering, because all transactions are public.** **But it is the instrument used in the deep/dark web for illegal payments.** Authorities, including the European Banking Authority the FBI, and the Financial Action Task Force of the G7 have expressed concerns that bitcoin may be used for money laundering. In early 2014, an operator of a U.S. bitcoin exchange, Charlie Shrem, was arrested for money laundering.Subsequently, he was sentenced to two years in prison for ”aiding and abetting an unlicensed money transmitting business”. Alexander Vinnik, an alleged owner of BTC-e was arrested in Greece July 25 of 2017 on $4 billion money laundering charges for ﬂouting anti-money laundering (AML) laws of the US. A report by UK’s Treasury and Home Oﬃce named ”UK national risk assessment of money laundering and terrorist ﬁnancing” (2015 October) found that, of the twelve methods examined in the report, bitcoin carries the lowest risk of being used for money laundering, with the most common money laundering method being the banks.

**Other illegal way to use Bitcoins are financial Ponzi schemes**. A Ponzi scheme is a form of fraud which lures investors and pays profits to earlier investors by using funds obtained from more recent investors. Investors may be led to believe that the profits are coming from product sales, or other means, and remain unaware that other investors are the source of profits. **A Ponzi scheme is able to maintain the illusion of a sustainable business as long as there continues to be new investors willing to contribute new funds and most of the investors do not demand full repayment and are willing to believe in the non-existent assets that they are purported to own. The scheme is named after Charles Ponzi, who became notorious for using the technique in the 1920s.** Ponzi's original scheme was based on the legitimate arbitrage of international reply coupons for postage stamps, but he soon began diverting new investors' money to make payments to earlier investors and himself.

**Cryptocurrencies have been employed by scammers attempting a new generation of Ponzi schemes.** For example, misuse of initial coin offerings, or "ICOs," on the Ethereum blockchain platform have been one such method. (per the Financial Times, "smart Ponzis"). The novelty of ICOs means that there is currently a lack of regulatory clarity on the classification of these financial devices, allowing scammers wide leeway to develop Ponzi schemes using these assets. More in detail, **economic bubbles are similar to a Ponzi scheme in that one participant gets paid by contributions from a subsequent participant (until inevitable collapse)**. A bubble involves ever-rising prices in an open market (for example stock, housing, cryptocurrency, or tulip bulbs) where prices rise because buyers bid more, and buyers bid more because prices are rising. **Bubbles are often said to be based on the "greater fool" theory**. As with the Ponzi scheme, the price exceeds the intrinsic value of the item, but unlike the Ponzi scheme, in most economic bubbles, there is no single person or group misrepresenting the intrinsic value. **Whereas Ponzi schemes will typically result in criminal charges after they are discovered by the authorities, economic bubbles do not typically involve unlawful activity, or even bad faith on the part of any participant.**

Following the collapse of a Ponzi scheme, the "innocent" beneficiaries will be liable to repay any such profits or donations for distribution to the victims. This typically does not happen in the case of an economic bubble, especially if it cannot be proven that the bubble was caused by anyone acting in bad faith. For instance, the Bitcoin Savings and Trust promised investors up to 7% weekly interest, and raised at least 700,000 bitcoins from 2011 to 2012. In July 2013, the U.S. Securities and Exchange Commission charged the company and its founder in 2013 ”with defrauding investors in a Ponzi scheme involving bitcoin”. In September 2014 the judge ﬁned Bitcoin Savings & Trust and its owner $40 million. **It is also used to pay the ransom of PC infected by viruses.**

**Consensus problem**

One of the problems to solve to have a cryptocurrency is the **Byzantine generals problem**. The term is derived from the Byzantine Generals’ Problem, where **actors must agree on a concerted strategy to avoid catastrophic system failure, but some of the actors are unreliable.** Byzantine fault tolerance has been also referred to with the phrases interactive consistency or source congruency, error avalanche, Byzantine agreement problem, Byzantine generals problem, and Byzantine failure. A Byzantine fault is any fault presenting diﬀerent symptoms to diﬀerent observers. A Byzantine failure is the loss of a system service due to a Byzantine fault in systems that require consensus.

**The objective of Byzantine fault tolerance is to be able to defend against failures of system components with or/and without symptoms that prevent other components of the system from reaching an agreement among themselves**, where such an agreement is needed for the correct operation of the system. Remaining correctly operational components of a Byzantine fault tolerant system will be able to continue providing the system’s service as originally intended, assuming there are suﬃcient accurately operating components to maintain the service. **Byzantine failures are considered the most general and most diﬃcult class of failures among the failure modes**.

The so-called fail-stop failure mode occupies the simplest end of the spectrum. Whereas fail-stop failure model simply means that the only way to fail is a node crash, detected by other nodes, Byzantine failures imply no restrictions, which means that the failed node can generate arbitrary data, pretending to be a correct one. Thus**, Byzantine failures can confuse failure detection systems, which makes fault tolerance diﬃcult. Despite the analogy, a Byzantine failure is not necessarily a security problem involving hostile human interference: it can arise purely from electrical faults.**

Byzantine refers to the Byzantine Generals’ Problem, an agreement problem, (described **by Leslie Lamport, Robert Shostak and Marshall Pease in their 1982 paper, ”The Byzantine Generals Problem”**), in which a group of generals, each commanding a portion of the Byzantine army, encircle a city. **These generals wish to formulate a plan for attacking the city. In its simplest form, the generals must decide only whether to attack or retreat.** Some generals may prefer to attack, while others prefer to retreat. The important thing is that every general agrees on a common decision, for a halfhearted attack by a few generals would become a rout and be worse than a coordinated attack or a coordinated retreat. By curiosity, this problem was originally named “The Albanian General Problem”. It was successively renamed as Byzantine for “politically correct reasons”.

**The problem is complicated by the presence of traitorous generals who may not only cast a vote for a suboptimal strategy, they may do so selectively**. For instance, if nine generals are voting, four of whom support attacking while four others are in favour of retreat, the ninth general may send a vote of retreat to those generals in favour of retreat, and a vote of attack to the rest. Those who received a retreat vote from the ninth general will retreat, while the rest will attack (which may not go well for the attackers). **The problem is complicated further by the generals being physically separated and having to send their votes via messengers who may fail to deliver votes or may forge false votes.**

**Byzantine errors were observed infrequently and at irregular points** during endurance testing for the newly constructed Virginia class submarines, at least through 2005 (when the issues were publicly reported). **A similar problem faces honeybee swarms. They have to ﬁnd a new home, and the many scouts and wider participants have to reach consensus about which of perhaps several candidate homes to ﬂy to.** And then they all have to ﬂy there, with their queen. The bees’ approach works reliably, but **when researchers oﬀer two hives, equally attractive by all the criteria bees apply, catastrophe ensues, the swarm breaks up, and all the bees die.**

Several solutions were described by Lamport, Shostak, and Pease in 1982. They began by noting that the Generals’ Problem can be reduced to solving a ”Commander and Lieutenants” problem where loyal Lieutenants must all act in unison and that their action must correspond to what the Commander ordered in the case that the Commander is loyal. The impossibility of dealing with one-third or more traitors ultimately reduces to proving that the one Commander and two Lieutenants problem cannot be solved, if the Commander is traitorous. **In 1999, Miguel Castro and Barbara Liskov introduced the ”Practical Byzantine Fault Tolerance” (PBFT) algorithm, which provides high-performance Byzantine state machine replication**, processing thousands of requests per second with sub-millisecond increases in latency.

**One of the reason of the success of the bitcoin is that its approach gives a solution to the consensus problem.** As already written, **the consensus problem is one of the fundamental and difficult problems in distributed computing** when it is necessary to achieve overall system reliability in the presence of a number of faulty processes. This often requires processes to agree on some data value that is needed during computation. Examples of applications of consensus   include whether to commit a transaction to a database (as in the case of bitcoins), agreeing on the identity of a subject,  choosing the right strategy in the case of swarm robotics where it is necessary the coordination of multiple robots, each one independent for the others.   It is supposed that a desired collective behaviour emerges from the interactions between the robots.

The consensus problem requires agreement among a number of processes (or agents) for a single data value. **Some of the processes (agents) may fail or be unreliable in other ways, so consensus protocols must be fault tolerant or resilient.** The processes must somehow put forth their candidate values, communicate with one another, and agree on a single consensus value. One approach to generating consensus is for all processes (agents) to agree on a majority value. In this context, a majority requires at least one more than half of available votes (where each process is given a vote). **However, one or more faulty processes may skew the resultant outcome such that consensus may not be reached or reached incorrectly. For instance in the so-called Sybil attack, the attacker subverts the reputation system of a peer-to-peer network  by creating a large number of pseudonymous   identities, using them to gain a disproportionately large influence.**

 **A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically**. This problem is strictly connected to **social choice problem, or voting theory**. This problem was considered **in France at the end of the absolutistic regime**. With the end of the monarchy at the instauration of the republic, it was natural o consider **the question what was the most efficient electoral system to represent the people’s will**. Quite surprisingly, the more obvious system, **the proportional system (any vote counts one) is not the best one. This was rigorously proved by Arrow in 1950 when in its celebrate Arrow's impossibility theorem,** proved the impossibility,   when voters have three or more distinct alternatives (options), that a no ranked voting electoral system (for instance the proportional system)  can correctly represent the  preferences of individuals into a community-wide ranking.

Even if this Theorem was proved only in the last century, this idea was already developed at the end of the 18th century by Condorcet and Borda with two different approaches. **Marie Jean Antoine Nicolas de Caritat, Marquis of Condorcet** was a French philosopher and mathematician. In 1785, Condorcet wrote an essay on the **application of analysis of the probability of decisions made on a majority vote.** This work stated the famous Condorcet paradox  which shows that majority preferences can become intransitive  with three or more options. I.e., it is possible for a certain electorate to express a preference for A over B, a preference for B over C, and a preference for C over A, all from the same set of ballots.**Condorcet proposed a pair-wise elections between all candidates in an election. In other words Condorcet proposed the same system used today to rank the soccer team in the Italian championship. This method is, more or less, implemented in the American election system with the primary system** (to reduce the choice among only two competitors) and the final ballot.

A completely alternative method was proposed by **Jean-Charles, chevalier de Borda**  a French mathematician, physicist, political scientist and sailor. **In 1770, Borda formulated a ranked preferential  voting system . The French Academy of Science  used Borda's method to elect its members for about two decades until 1801. The Borda count is in use today in some academic institutions, competitions and several political jurisdictions (Iceland and Slovenia have a similar system).**  The Borda count determines the winner of an election by giving each candidate, for each ballot, a number of points corresponding to the number of candidates ranked lower. Once all votes have been counted the option or candidate with the most points is the winner.

Let us explain it with an example. Consider the last political Italian elections and, for the sake of simplicity, consider only four parties: Lega, Forza Italia, Movimento Cinque Stelle and Partito Democratico. For instance, the Lega Supporters ranked obviously as first Lega, then in second position Forza Italia, Movimento 5 Stelle is third and fourth is Partito Democratico. So Lega has the following points: the numbers of its votes multiplied by four, the number of Forza Italia votes multiplied by three, the number of M5S votes multiplied by two and the numbers of PD votes. Repeating this argument for all the four main parties, one find that **the “Borda” winner of the last Italian election was Lega, followed by M5S** and FI. A very different result compared with the actual results. By curiosity, **the Republican Roman senate was using a method very similar to the one introduced by Borda.**

If it is so complicate to find a satisfactory system for political election, one can imagine the difficulty to find a satisfactory approach in the case of distributed computing. **Bitcoin use the so called roof-of-work**. Actually, the bitcoin network works in parallel to generate a chain of Hashcash style proof-of-work (known as mining). The proof-of-work chain is the key to overcome Byzantine failures and to reach a coherent global view of the system state. Obviously this approach was used in other context, too. For instance some aircraft systems, such as the Boeing 777 Aircraft Information Management System the Boeing 777 ﬂight control system, and the Boeing 787 ﬂight control systems, use Byzantine fault tolerance. Because these are real-time systems, their Byzantine fault tolerance solutions must have very low latency. For example, SAFEbus can achieve Byzantine fault tolerance within the order of a microsecond of added latency.

Among instruments to get the consensus, we recall **Paxos is a family of protocols for solving consensus in a network of unreliable processors.** Consensus is the process of agreeing on one result among a group of participants. This problem becomes diﬃcult when the participants or their communication medium may experience failures. Consensus protocols are the basis for the state machine replication approach to distributed computing, as suggested by Leslie Lamport and surveyed by Fred Schneider. State machine replication is a technique for converting an algorithm into a fault-tolerant, distributed implementation. Ad-hoc techniques may leave important cases of failures unresolved. The principled approach proposed by Lamport et al. ensures all cases are handled safely. **The Paxos protocol was ﬁrst published in 1989 and named after a ﬁctional legislative consensus system used on the Paxos island in Greece.** It was later published as a journal article in 1998.

**III LESSON: CAP THEOREM AND A BRIEF HISTORY OF CRYPTOGRAPHY**

**CAP Theorem**

In theoretical computer science, the CAP theorem, also named Brewer’s theorem after computer scientist Eric Brewer, states that it is impossible for a distributed data store to simultaneously provide more than two out of the following three guarantees:

**Consistency**: Every read receives the most recent write or an error.

**Availability:** Every request receives a (non-error) response without guarantee that it contains the most recent write

**Partition tolerance**: The system continues to operate despite an arbitrary number of messages being dropped (or delayed) by the network between nodes

**In other words, the CAP theorem states that in the presence of a network partition, one has to choose between consistency and availability**. No distributed system is safe from network failures, thus network partitioning generally has to be tolerated. In the presence of a partition, one is then left with two options: consistency or availability. When choosing consistency over availability, the system will return an error or a time-out if particular information cannot be guaranteed to be up to date due to network partitioning. When choosing availability over consistency, the system will always process the query and try to return the most recent available version of the information, even if it cannot guarantee it is up to date due to network partitioning. **In the absence of network failure - that is, when the distributed system is running normally - both availability and consistency can be satisﬁed**.

**Cryptography: its origin**

**Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago.** Some clay tablets from Mesopotamia somewhat later are clearly meant to protect information - one dated near 1500 BCE was found to encrypt a craftsman's recipe for pottery glaze, presumably commercially valuable. Furthermore, Hebrew scholars made use of simple monoalphabetic substitution ciphers beginning perhaps around 500 to 600 BCE. In India around 400 BCE to 200 CE, the art of understanding writing in cypher, and the writing of words in a peculiar way **was documented in the Kama Sutra for the purpose of communication between lovers.** The ancient Greeks used cryptography. The scytale transposition cipher was used by the Spartan military. **Herodotus tells us of secret messages** physically concealed beneath wax on wooden tablets or **as a tattoo on a slave's head concealed by regrown hair**, although these are not properly examples of cryptography per se as the message, once known, is directly readable; this is known as steganography. The Romans knew cryptography (i.e the famous **Caesar cipher** and its variations).

 **The modern cryptology originated among the Arabs, the first people to systematically document cryptanalytic methods**. The invention of the frequency-analysis technique for breaking monoalphabetic substitution ciphers, by Al-Kindi, an Arab mathematician sometime around AD 800 proved to be the single most significant cryptanalytic advance until World War II. Al-Kindi wrote a book on cryptography entitled Manuscript for the Deciphering Cryptographic Messages, in which he **described the first cryptanalytic techniques, including some for polyalphabetic ciphers, cipher classification, Arabic phonetics and syntax, and most importantly, gave the first descriptions on frequency analysis**. Ahmad al-Qalqashandi (AD 1355–1418) wrote a 14-volume encyclopedia which included a section on cryptology. This information was attributed to Ibn al-Durayhim who lived from AD 1312 to 1361, but whose writings on cryptography have been lost. **The list of ciphers in this work included both substitution and transposition, and for the first time, a cipher with multiple substitutions for each plaintext letter**. Also traced to Ibn al-Durayhim is an exposition on and worked example of cryptanalysis, including the use of tables of letter frequencies and sets of letters which cannot occur together in one word.

The earliest example of the homophonic substitution cipher is the one used by **Duke of Mantua in the early 1400s.** Homophonic cipher replaces each letter with multiple symbols depending on the letter frequency. The cipher is ahead of the time because it combines monoalphabetic and polyalphabetic features.

Essentially all ciphers remained vulnerable to the cryptanalytic technique of frequency analysis until the development of the polyalphabetic cipher, and many remained so thereafter. The polyalphabetic cipher was most clearly explained by **Leon Battista Alberti around the year AD 1467, for which he was called the "father of Western cryptology"**. **Johannes Trithemius, in his work Poligraphia**, invented the tabula recta, a critical component of the Vigenère cipher. Trithemius also wrote the Steganographia. **The French cryptographer Blaise de Vigenère devised a practical polyalphabetic system** which bears his name, the Vigenère cipher.

**In Europe, cryptography became (secretly) more important as a consequence of political competition and religious revolution**. For instance, in Europe during and after the Renaissance, citizens of the various Italian states - the Papal States and the Roman Catholic Church included- were responsible for rapid proliferation of cryptographic techniques, few of which reflect understanding (or even knowledge) of Alberti's polyalphabetic advance. 'Advanced ciphers', even after Alberti, weren't as advanced as their inventors / developers / users claimed (and probably even themselves believed). They were regularly broken. This over-optimism may be inherent in cryptography, for it was then - and remains today - fundamentally difficult to accurately know how vulnerable one's system actually is. In the absence of knowledge, guesses and hopes, predictably, are common. **Cryptography, cryptanalysis, and secret-agent/courier betrayal featured in the Babington plot during the reign of Queen Elizabeth I which led to the execution of Mary, Queen of Scots**. Robert Hooke suggested in the chapter Of Dr. Dee's Book of Spirits, that John Dee made use of Trithemian steganography, to conceal his communication with Queen Elizabeth I.

**The chief cryptographer of King Louis XIV of France was Antoine Rossignol** and he and his family created what is known as the Great Cipher because it remained unsolved from its initial use until 1890, when French military cryptanalyst, Étienne Bazeries solved it. **An encrypted message from the time of the Man in the Iron Mask (decrypted just prior to 1900 by Étienne Bazeries) has shed some, regrettably non-definitive, light on the identity of that real, if legendary and unfortunate, prisoner** .Outside of Europe, after the Mongols brought about the end of the Muslim Golden Age, cryptography remained comparatively undeveloped. Cryptography in Japan seems not to have been used until about 1510, and advanced techniques were not known until after the opening of the country to the West beginning in the 1860s.

**Cryptography during the two World Wars**

Although cryptography has a long and complex history, it wasn't until the 19th century that it developed anything more than ad hoc approaches to either encryption or **cryptanalysis (the science of finding weaknesses in crypto systems). Examples of the latter include Charles Babbage's Crimean War era work** on mathematical cryptanalysis of polyalphabetic ciphers, redeveloped and published somewhat later by the Prussian **Friedrich Kasiski**. Understanding of cryptography at this time typically consisted of hard-won rules of thumb; see, for example**, Auguste Kerckhoffs'** cryptographic writings in the latter 19th century. **Edgar Allan Poe** used systematic methods to solve ciphers in the 1840s. He later wrote an essay on methods of cryptography which proved useful as an introduction for novice British cryptanalysts attempting to break German codes and ciphers during World War I, and a famous story, The Gold-Bug, in which cryptanalysis was a prominent element.

**Cryptography, and its misuse, were involved in the execution of Mata Hari and in Dreyfus' conviction and imprisonment**, both in the early 20th century. Cryptographers were also involved in exposing the machinations which had led to the Dreyfus affair; Mata Hari, in contrast, was shot. In World War **I the Admiralty's Room 40 broke German naval codes** and played an important role in several naval engagements during the war, notably in detecting major German sorties into the North Sea that led to the battles of Dogger Bank and Jutland as the British fleet was sent out to intercept them. However its most important contribution was probably in decrypting **the Zimmermann Telegram, a cable from the German Foreign Office sent via Washington to its ambassador Heinrich von Eckardt in Mexico** which played a major part in bringing the United States into the war. In 1917, **Gilbert Vernam** proposed a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cyphertext. This led to the development of electromechanical devices as cipher machines, and to **the only unbreakable cipher, the onetime pad** . During the 1920s, Polish naval-officers assisted the Japanese military with code and cipher development**. Mathematical methods proliferated in the period prior to World War II** (notably in William F. Friedman's application of statistical techniques to cryptanalysis and cipher development and in Marian Rejewski's initial break into the German Army's version of the Enigma system in 1932).

**By World War II, mechanical and electromechanical cipher machines were in wide use**, although - where such machines were impractical - manual systems continued in use. Great advances were made in both cipher design and cryptanalysis, all in secrecy. Information about this period has begun to be declassified as the official British 50-year secrecy period has come to an end, as US archives have slowly opened, and as assorted memoirs and articles have appeared. **The Germans made heavy use, in several variants, of an electromechanical rotor machine known as Enigma**. Mathematician Marian Rejewski, at Poland's Cipher Bureau, in December 1932 deduced the detailed structure of the German Army Enigma, using mathematics and limited documentation supplied by Captain Gustave Bertrand of French military intelligence. Rejewski and his mathematical Cipher Bureau colleagues, Jerzy Różycki and Henryk Zygalski, continued reading Enigma and keeping pace with the evolution of the German Army machine's components and encipherment procedures. As the Poles' resources became strained by the changes being introduced by the Germans, and as war loomed, the Cipher Bureau, on the Polish General Staff's instructions, on 25 July 1939, at Warsaw, initiated French and British intelligence representatives into the secrets of Enigma decryption.

Soon after the Invasion of Poland by Germany on 1 September 1939, key Cipher Bureau personnel were evacuated southeast ward; on 17 September, as the Soviet Union attacked Poland from the East, they crossed into Romania. From there they reached Paris, France; at PC Bruno, near Paris, they continued breaking Enigma, collaborating with British cryptologists at Bletchley Park as the British got up to speed on breaking Enigma. In due course, **the British cryptographers - whose ranks included many chess masters and mathematics dons such as Gordon Welchman, Max Newman, and Alan Turing** (the conceptual founder of modern computing) - substantially advanced the scale and technology of Enigma decryption. German code breaking in World War II also had some success, most importantly by breaking the Naval Cypher No. 3. This enabled them to track and sink Atlantic convoys. It was only Ultra intelligence that finally persuaded the admiralty to change their codes in June 1943. This is surprising given the success of the British Room 40 code breakers in the previous world war.

**At the end of the War, on 19 April 1945, Britain's top military officers were told that they could never reveal that the German Enigma cipher had been broken because it would give the defeated enemy the chance to say they "were not well and fairly beaten".** US Navy cryptographers (with cooperation from British and Dutch cryptographers after 1940) broke into several Japanese Navy crypto systems. **The break into one of them, JN-25, famously led to the US victory in the Battle of Midway**; and to the publication of that fact in the Chicago Tribune shortly after the battle, though the Japanese seem not to have noticed for they kept using the JN-25 system. A US Army group, the SIS, managed to break the highest security Japanese diplomatic cipher system (an electromechanical 'stepping switch' machine called Purple by the Americans) even before World War II began. The Americans referred to the intelligence resulting from cryptanalysis, perhaps especially that from the Purple machine, as 'Magic'. The British eventually settled on 'Ultra' for intelligence resulting from cryptanalysis, particularly that from message traffic protected by the various Enigmas. An earlier British term for Ultra had been 'Boniface' in an attempt to suggest, if betrayed, that it might have an individual agent as a source.

**The German military also deployed several mechanical attempts at a one-time pad. Bletchley Park called them the Fish ciphers**, and Max Newman and colleagues designed and deployed the Heath Robinson, and then the world's first programmable digital electronic computer, the Colossus, to help with their cryptanalysis. The German Foreign Office began to use the one-time pad in 1919; some of this traffic was read in World War II partly as the result of recovery of some key material in South America that was discarded without sufficient care by a German courier. The Japanese Foreign Office used a locally developed electrical stepping switch based system (called Purple by the US), and also had used several similar machines for attaches in some Japanese embassies. One of the electrical stepping switch based systems referred to earlier as Purple was called the 'M-machine' by the US, another was referred to as 'Red'. All were broken, to one degree or another, by the Allies. Allied cipher machines used in World War II included the British TypeX and the American SIGABA; both were electromechanical rotor designs similar in spirit to the Enigma, albeit with major improvements. Neither is known to have been broken by anyone during the War. The Poles used the Lacidamachine, but its security was found to be less than intended (by Polish Army cryptographers in the UK), and its use was discontinued. US troops in the field used the M-209 and the still less secure M-94 family machines. **British SOE agents initially used 'poem ciphers' (memorized poems were the encryption/decryption keys)**, but later in the War, they began to switch to one-time pads. The VIC cipher (used at least until 1957 in connection with Rudolf Abel's NY spy ring) was a very complex hand cipher, and is claimed to be the most complicated known to have been used by the Soviets.

**Modern cryptography**

**Claude E. Shannon** is considered by many to be the father of mathematical cryptography. Shannon worked for several years at Bell Labs, and during his time there, he produced an article **entitled "A mathematical theory of cryptography".** This article was written in 1945 and eventually was published in the Bell System Technical Journal in 1949. It is commonly accepted that this paper was the starting point for development of modern cryptography. Shannon was inspired during the war to address the problems of cryptography because secrecy systems furnish an interesting application of communication theory. **Shannon identified the two main goals of cryptography: secrecy and authenticity**. His focus was on exploring secrecy and thirty-five years later, G.J. Simmons would address the issue of authenticity. Shannon wrote a further article entitled "A mathematical theory of communication" which highlights one of the most significant aspects of his work: **cryptography's transition from art to science**. In his works, Shannon described **the two basic types of systems for secrecy. The first are those designed with the intent to protect against hackers and attackers who have infinite resources with which to decode a message** (theoretical secrecy, now unconditional security), and the **second are those designed to protect against hackers and attacks with finite resources** with which to decode a message (practical secrecy, now computational security).

 Most of Shannon's work focused around theoretical secrecy; here, Shannon introduced a definition for the **"unbreakability"** of a cipher. If a cipher was determined "unbreakable", it was considered to have "perfect secrecy". In proving "perfect secrecy", Shannon determined **that this could only be obtained with a secret key whose length given in binary digits was greater than or equal to the number of bits contained in the information being encrypted.** Furthermore, Shannon developed the "unicity distance", defined as the "amount of plaintext that… determines the secret key." Shannon's work influenced further cryptography research in the 1970s, as the public-key cryptography developers, M. E. Hellman and W. Diffie cited Shannon's research as a major influence. His work also impacted modern designs of secret-key ciphers. At the end of Shannon's work with cryptography, progress slowed until Hellman and Diffie introduced their paper involving "public-key cryptography".

**Until the 1970s, secure cryptography was largely the preserve of governments**. Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. These keys convert the messages and data into "digital gibberish" through encryption and then return them to the original form through decryption. In general, the longer the key is, the more difficult it is to crack the code. This holds true because deciphering an encrypted message by brute force would require the attacker to try every possible key. To put this in context, each binary unit of information, or bit, has a value of 0 or 1. An 8-bit key would then have 256 or 28 possible keys. A 56-bit key would have 256, or 72 quadrillion, possible keys to try and decipher the message. With modern technology, cyphers using keys with these lengths are becoming easier to decipher. DES, an early US Government approved cypher, has an effective key length of 56 bits, and test messages using that cypher have been broken by brute force key search. However, as technology advances, so does the quality of encryption**. Since World War II, one of the most notable advances in the study of cryptography is the introduction of the asymmetric key cyphers** (sometimes termed public-key cyphers). These are algorithms which use two mathematically related keys for encryption of the same message. Some of these algorithms permit publication of one of the keys, due to it being extremely difficult to determine one key simply from knowledge of the other.

**IV LESSON: MODERN CRIPTOGRAPHY AND ELLIPTIC CURVES**

**The mid-1970s saw two major public (i.e., non-secret) advances. First was the publication of the draft Data Encryption Standard in the U.S. Federal Register on 17 March 1975**. The proposed DES cipher was submitted by a research group at IBM, at the invitation of the National Bureau of Standards (now NIST), in an effort to develop secure electronic communication facilities for businesses such as banks and other large financial organizations. After advice and modification by the NSA, acting behind the scenes, it was adopted and published as a Federal Information Processing Standard Publication in 1977 (currently at FIPS 46-3). **DES was the first publicly accessible cipher to be 'blessed' by a national agency such as the NSA.** The release of its specification by NBS stimulated an explosion of public and academic interest in cryptography. **The aging DES was officially replaced by the Advanced Encryption Standard (AES) in 2001** when NIST announced FIPS 197. After an open competition**, NIST selected Rijndael, submitted by two Belgian cryptographers**, to be the AES. DES, and more secure variants of it (such as Triple DES), are still used today, having been incorporated into many national and organizational standards. However, its 56-bit key-size has been shown to be insufficient to guard against brute force attacks (one such attack, undertaken by the cyber civil-rights group Electronic Frontier Foundation in 1997, succeeded in 56 hours.) As a result, use of straight DES encryption is now without doubt insecure for use in new cryptosystem designs, and **messages protected by older cryptosystems using DES, and indeed all messages sent since 1976 using DES, are also at risk**. Regardless of DES' inherent quality, the DES key size (56-bits) was thought to be too small by some even in 1976, perhaps most publicly by Whitfield Diffie. There was suspicion that government organizations even then had sufficient computing power to break DES messages; clearly others have achieved this capability.

**The second development, in 1976, was** perhaps even more important, for it fundamentally changed the way cryptosystems might work. This **was the publication of the paper New Directions in Cryptography by Whitfield Diffie and Martin Hellman**. It introduced a radically new method of distributing cryptographic keys, which went far toward solving one of the fundamental problems of cryptography, key distribution, and has become known as Diffie - Hellman key exchange. The article also stimulated the almost immediate public development of a new class of enciphering algorithms, the asymmetric key algorithms. **Prior to that time, all useful modern encryption algorithms had been symmetric key algorithms, in which the same cryptographic key is used with the underlying algorithm by both the sender and the recipient, who must both keep it secret.** All of the electromechanical machines used in World War II were of this logical class, as were the Caesar ciphers and essentially all cipher systems throughout history. The 'key' for a code is, of course, the codebook, which must likewise be distributed and kept secret, and so shares most of the same problems in practice.

Of necessity**, the key in every such system had to be exchanged between the communicating parties in some secure way prior to any use of the system** (the term usually used is 'via a secure channel') such as a **trustworthy courier with a briefcase handcuffed to a wrist, or face-to-face contact, or a loyal carrier pigeon**. This requirement is never trivial and very rapidly becomes unmanageable as the number of participants increases, or when secure channels aren't available for key exchange, or when, as is sensible cryptographic practice, keys are frequently changed. In particular, if messages are meant to be secure from other users, a separate key is required for each possible pair of users. A system of this kind is known as a secret key, or symmetric key cryptosystem. **D-H key exchange (and succeeding improvements and variants) made operation of these systems much easier, and more secure, than had ever been possible before in all of history**. In contrast, asymmetric key encryption uses a pair of mathematically related keys, each of which decrypts the encryption performed using the other. **Some, but not all, of these algorithms have the additional property that one of the paired keys cannot be deduced from the other by any known method other than trial and error. An algorithm of this kind is known as a public key or asymmetric key system**. Using such an algorithm, only one key pair is needed per user. By designating one key of the pair as private (always secret), and the other as public (often widely available), no secure channel is needed for key exchange. So long as the private key stays secret, the public key can be widely known for a very long time without compromising security, making it safe to reuse the same key pair indefinitely.

For two users of an asymmetric key algorithm to communicate securely over an insecure channel, each user will need to know their own public and private keys as well as the other user's public key. Take this basic scenario**: Alice and Bob each have a pair of keys they've been using for years with many other users. At the start of their message, they exchange public keys, unencrypted over an insecure line. Alice then encrypts a message using her private key, and then re-encrypts that result using Bob's public key.** The double-encrypted message is then sent as digital data over a wire from Alice to Bob. Bob receives the bit stream and decrypts it using his own private key, and then decrypts that bit stream using Alice's public key. If the final result is recognizable as a message, Bob can be confident that the message actually came from someone who knows Alice's private key (presumably actually her if she's been careful with her private key), and that anyone eavesdropping on the channel will need Bob's private key in order to understand the message.

**Asymmetric algorithms rely for their effectiveness on a class of problems in mathematics called one-way functions, which require relatively little computational power to execute, but vast amounts of power to reverse, if reversal is possible at all. A classic example of a one-way function is multiplication of very large prime numbers.** It's fairly quick to multiply two large primes, but very difficult to find the factors of the product of two large primes. Because of the mathematics of one-way functions, most possible keys are bad choices as cryptographic keys; only a small fraction of the possible keys of a given length are suitable, and so asymmetric algorithms require very long keys to reach the same level of security provided by relatively shorter symmetric keys. The need to both generate the key pairs, and perform the encryption/decryption operations make asymmetric algorithms computationally expensive, compared to most symmetric algorithms. Since symmetric algorithms can often use any sequence of (random, or at least unpredictable) bits as a key, a disposable session key can be quickly generated for short-term use. **Consequently, it is common practice to use a long asymmetric key to exchange a disposable, much shorter (but just as strong) symmetric key. The slower asymmetric algorithm securely sends a symmetric session key, and the faster symmetric algorithm takes over for the remainder of the message.**

**Asymmetric key cryptography, Diffie - Hellman key exchange, and the best known of the public key / private key algorithms (i.e., what is usually called the RSA algorithm), all seem to have been independently developed at a UK intelligence agency** before the public announcement by Diffie and Hellman in 1976. GCHQ has released documents claiming they had developed public key cryptography before the publication of Diffie and Hellman's paper. Various classified papers were written at GCHQ during the 1960s and 1970s which eventually led to schemes essentially identical to RSA encryption and to Diffie - Hellman key exchange in 1973 and 1974. Some of these have now been published, and the inventors (James H. Ellis, Clifford Cocks, and Malcolm Williamson) have made public (perhaps, some of) their work. **Beginning around 1990, the use of the Internet for commercial purposes and the introduction of commercial transactions over the Internet called for a widespread standard for encryption**. Before the introduction of the Advanced Encryption Standard (AES), information sent over the Internet, such as financial data, was encrypted if at all, most commonly using the Data Encryption Standard (DES).. Around the late 1990s to early 2000s, the use of public-key algorithms became a more common approach for encryption, and soon a hybrid of the two schemes became the most accepted way for e-commerce operations to proceed. **Additionally, the creation of a new protocol known as the Secure Socket Layer, or SSL, led the way for online transactions to take place. Transactions ranging from purchasing goods to online bill pay and banking used SSL. Furthermore, as wireless Internet connections became more common among households, the need for encryption grew, as a level of security was needed in these everyday situations.**

As we will say also later, when we will describe how bitcoins works,  **hashing is a common technique** used in cryptography to encode information quickly using typical algorithms. **Generally, an algorithm is applied to a string of text, and the resulting string becomes the "hash value".** This creates a "digital fingerprint" of the message, as the specific hash value is used to identify a specific message**. The output from the algorithm is also referred to as a "message digest" or a "check sum".** Hashing is good for determining if information has been changed in transmission. If the hash value is different upon reception than upon sending, there is evidence the message has been altered. Once the algorithm has been applied to the data to be hashed, the hash function produces a fixed-length output. Essentially, anything passed through the hash function should resolve to the same length output as anything else passed through the same hash function. It is important to note that hashing is not the same as encrypting. **Hashing is a one-way operation that is used to transform data into the compressed message digest. Additionally, the integrity of the message can be measured with hashing.** Conversely, encryption is a two-way operation that is used to transform plaintext into cipher-text and then vice versa. In encryption, the confidentiality of a message is guaranteed

Hash functions can be used to verify digital signatures, so that when signing documents via the Internet, the signature is applied to one particular individual. Much like a hand-written signature, these signatures are verified by assigning their exact hash code to a person. Furthermore, hashing is applied to passwords for computer systems. **Hashing for passwords began with the UNIX operating system**. A user on the system would first create a password. That password would be hashed, using an algorithm or key, and then stored in a password file. This is still prominent today, as web applications that require passwords will often hash user's passwords and store them in a database. As a natural consequence, **the public developments of the 1970s broke the near monopoly on high quality cryptography held by government organizations. For the first time ever, those outside government organizations had access to cryptography not readily breakable by anyone (including governments).** Considerable controversy, and conflict, both public and private, began more or less immediately, sometimes called the crypto wars. They have not yet subsided. In many countries, for example, export of cryptography is subject to restrictions. Until 1996 export from the U.S. of cryptography using keys longer than 40 bits (too small to be very secure against a knowledgeable attacker) was sharply limited. **As recently as 2004, former FBI Director Louis Freeh, testifying before the 9/11 Commission, called for new laws against public use of encryption**.

One of the most significant people favouring strong encryption for public use was Phil Zimmermann. He wrote and then in 1991 released PGP (Pretty Good Privacy), a very high quality crypto system. He distributed a freeware version of PGP when he felt threatened by legislation then under consideration by the US Government that would require backdoors to be included in all cryptographic products developed within the US. His system was released worldwide shortly after he released it in the US, and that began a long criminal investigation of him by the US Government Justice Department for the alleged violation of export restrictions. The Justice Department eventually dropped its case against Zimmermann, and the freeware distribution of PGP has continued around the world. PGP even eventually became an open Internet standard . While modern ciphers like AES and the higher quality asymmetric ciphers are widely considered unbreakable, poor designs and implementations are still sometimes adopted and there have been important cryptanalytic breaks of deployed crypto systems in recent years. Notable examples of broken crypto designs include the first Wi-Fi encryption scheme WEP, the Content Scrambling System used for encrypting and controlling DVD use, the A5/1 and A5/2 ciphers used in GSM cell phones, and the CRYPTO1 cipher used in the widely deployed MIFARE Classic smart cards from NXP Semiconductors, a spun off division of Philips Electronics. All of these are symmetric ciphers. **Thus far, not one of the mathematical ideas underlying public key cryptography has been proven to be 'unbreakable', and so some future mathematical analysis advance might render systems relying on them insecure. While few informed observers foresee such a breakthrough, the key size recommended for security as best practice keeps increasing as increased computing power required for breaking codes becomes cheaper and more available**. In the sequel, we consider cryptographic systems based on elliptic curves that are the one used by bitcoins.

**Elliptic curves**

**Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over ﬁnite ﬁelds.** ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois ﬁelds) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme**. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is diﬃcult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that ﬁnding the discrete logarithm of a random elliptic curve** element with respect to a publicly known base point is infeasible: this is the ”elliptic curve discrete logarithm problem” (ECDLP). The security of elliptic curve cryptography depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the diﬃculty of the problem.

For current cryptographic purposes, **an elliptic curve** is a plane curve over a ﬁnite ﬁeld (rather than the real numbers) which consists of the points **satisfying the equation**

y2 = x3 + ax + b,

along with a distinguished point at inﬁnity. In the mathematics of the real numbers, the logarithm logba is a number x such that bx = a, for given numbers a and b. Analogously, in any group G, powers bk can be deﬁned for all integers k, and the discrete logarithm logba is an integer k such that bk = a**. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005.**

**The curve used by Bitcoin, secp256k1**, in the normal Weierstrass form has equation y2 = x3 + 7. The elliptic curve can take characteristic shapes in the plane according to its coeﬃcients, but each one is symmetrical with respect to the abscissa axis, since for each value of x there will be a positive and a negative value for y, that is: y = ±(x3 + ax + b)(1/2) . In cryptography, curves are used on which some algebraic properties can be deﬁned with respect to an internal composition operation, therefore **only non-singular curves will be taken into consideration, discarding all those curves with cusps or with self-intersections**

To verify the non-singularity of the curve, it is necessary to impose that its determinant is diﬀerent from 0, i.e. that the inequality exists: 4a3 + 27b2 different from 0 The points of a non-singular curve, combined with a special element 0 called point to inﬁnity or zero point, represent a set G, deﬁned in this way:

G = {(x,y) ∈R2|y2 = x3 + ax + b, 4a3 + 27b2 different from 0}∪{0}

**A commutative, or abelian, group is a non-empty set on which a · binary operation is deﬁned** to satisfy certain properties:

1. the set is closed with respect to the operation, i.e. if a and b belong to the set G then also c = a·b belongs to G;

2. the operation respects the associative property, or (a·b)·c = a·(b·c);

3. there is a 0 element, called identity element, such that a·0 = a and 0·a = a for every a;

4. each element has its inverse, that is, for every a, there exists b such that a·b = 0;

5. the operation respects the commutative property, or a·b = b·a for each a and b belonging to the set.

 **V LESSON: MORE ABOUT ELLIPTIC CURVES. AN INTRODUCTION TO QUANTUM COMPUTING**

**A group that contains a ﬁnite number of elements is called a ﬁnite group and the number of elements in the group is the group order, otherwise the group is called an inﬁnite group**. On a G group you can deﬁne the operation of elevation to power as the repeated application of the group operator, so a3 = a·a·a. A G group is called cyclic if each element of G is a power ak of a ﬁxed element a ∈ G, with k ∈ N, in this case it is he says that the element a generates the group G or that is a generator of G, moreover a cyclic group is always abelian and can be ﬁnite or inﬁnite. In the case of elliptic curves, the composition operation is the sum, indicated with the symbol +.

Moreover:

 - the **inverse** of a point P(xP,yP) is deﬁned as the point −P(xP,−yP) symmetric of P with respect to the axis x;

- the **identity element** is represented by the point to inﬁnity, or zero point 0 for which is worth 0 = −0 and for every point P belonging to G we have P + 0 = 0 + P = P;

- the **sum operation**, indicated with + is deﬁned by the rule P + Q + R = 0, with P,Q and R belonging to the set G and is aligned.

**The elements of the group can be represented as points on the Cartesian plane** and also the law of internal composition can be interpreted in a geometric way, establishing that if three points of the curve lie on the same line, or are aligned, their sum is zero. As we have to do with abelian group, it is guaranteed that each element has an inverse element with respect to the sum and that the operation of sum has the commutative property, so that the rule for the sum can be rewritten as P + Q = −R , where P,Q and R are aligned points. To calculate the sum between two points P and Q belonging to the curve we must draw a straight line between them until you ﬁnd a third intersection point R, the result of the sum will be the inverse of the point of intersection −R, symmetric of R with respect to the x axis.

Depending on the combination between the line passing through the two points and the curve, **we can deﬁne the sum in various way:**

1. if one of the two addends is the zero point, we cannot draw any line, since 0 does not belong to the curve, but by deﬁnition of element identity we can write P + 0 = P;

2. If one of the two addends is the inverse of the other, then the line passing between the two addends is a vertical line and does not intersect the curve at any point, but by deﬁnition of the inverse element we will have P + (−P) = 0;

3. if the two addends P and Q coincide, then P = Q and for them pass inﬁnite lines, among these we choose the tangent line to the curve passing through the point P, until you ﬁnd the intersection R with the curve, at this point we will have P + P = −R;

**The algebraic treatment of the sum proceeds in a similar way with respect the geometric version with various possible cases.** The cases for which the result descends directly from the deﬁnition of element identity P + 0 = P, and inverse element that is P + (−P) = 0, are trivial. In the case where P and Q are two non-symmetrical, non-null and distinct points, we have that the line that unites them has an angular coeﬃcient:

m = (yP −yQ)/( xP −xQ)

**The point of intersection between the line passing through the two points and the elliptic curve is a third point** R = (xR,yR) whose coordinates are deﬁned in this way: xR = m2 −xP −xQ, yR = yP + m×(xR −xP)

That is P + Q = −R where −R = (xR,−yR).

In the particular case where **we want to deﬁne the sum P + P we have to use the tangent to the curve** in point P and it is necessary to use the formula of the ﬁrst derivative with respect to x of the curve equation:

m = (3x2 P + a)/( 2yP)

We have seen that the set of points belonging to an elliptic curve, with the addition of the point to inﬁnity, constitutes, with respect to the previously deﬁned sum operation, an abelian group. We have formalized the details of the summing operation between two points belonging to the curve, this allows us to deﬁne a scalar multiplication operation of a point P belonging to the curve, for a natural number: nP = P + P ···+P for n times. **The multiplication of an element of the group for a scalar, that is the repeated application of the sum operator**, by deﬁnition represents the elevation to power within the group G, or P3 = 3P = P + P + P and **the inverse of this operation will be called logarithm on elliptic curves**.

Based on the algebraic formulas introduced previously for the sum of two points, we can perform the previous multiplication by making n−1 sum operations, actually, with the use of appropriate algorithms we can do much better . **One of the algorithms that can be used to eﬃciently implement the scalar multiplication operation is the double and add algorithm.** Given the product n\*P, with n ∈ N and P ∈ G, a generic scalar n can be written as the sum n0 + 2n1 + 22n2 ···+2mnm, where [n0, ···,nm] ∈{0,1} and m + 1 is the number of digits of the binary representation of n. Suppose we want to multiply the generic point P for 151, whose binary representation is 100101112, then we can write:

151\*P = 27P + 24P + 22P + 21P + 20P

**The double and add algorithm tells us:**

initialize the result Q to 0;

with i = 0, since d0 = 1 we add P to Q and store the result in Q and double P;

with i = 1, since d1 = 1 we add P to Q and store the result in Q and double P;

with i = 2, since d2 = 1 we add P to Q and store the result in Q and double P;

with i = 3, since d3 = 0 we do not execute any sum, but we double P;

with i = 4, since d4 = 1 we add P to Q and store the result in Q and double P;

with i = 5, since d5 = 0 we do not execute any sum, but we double P;

with i = 6, since d6 = 0 we do not execute any sum, but we double P;

 with i = 7, since d7 = 1 we add P to Q and store the result in Q and double P;

 no binary digits of n are left to be taken into account, then returns Q.

**The algorithm gives the result of multiplication by executing 5 sums and 7 multiplications.** For each iteration of the loop this algorithm performs a summing operation, or alternatively a summing operation followed by another summing operation (doubling P), the loop is executed as many times as the binary digits of n, this leads us to **estimate a cost of O(logn).** So far we have talked about elliptic curves in which the variables and the coeﬃcients belong to the real numbers, but **in their cryptographic application both the variables and the coeﬃcients are restricted to the elements of a ﬁnite ﬁeld**. In mathematics, a ﬁnite ﬁeld, or Galois ﬁeld, is a ﬁeld with a ﬁnite number p­n of elements, with p prime number and is often denoted as Z(pn) or GF(pn).

**The security of elliptic curve cryptography depends on the diﬃculty with which it is possible to perform the inverse operation**, i.e. to determine n when n\*P and P are given. This problem is called the discrete logarithm of the elliptic curve and it is a problem that is considered hard. **Currently the fastest known technique for calculating the logarithm is called the Pollard rho method. Designed by John Pollard in 1975, it was used in 1981 to factor Fermat’s eighth number issue** (a Fermat number, named after Pierre de Fermat who ﬁrst studied them, is a positive integer of the form Fn = (22)n + 1. It was conjectured that all the Fermat number were prime number, conjecture that was proved to be false) **It is a probabilistic algorithm, in the sense that it does not guarantee to produce a result.**

In reality **there are some elliptic curves for which it is possible to ﬁnd speciﬁc algorithms that solve the discrete logarithm in polynomial time**, such curves are not suitable for cryptographic uses and are therefore called weak. The possibility that some curves are intrinsically weak to a cryptographic analysis imposes several questions related to the trust that it is legitimate to place in objects of this type. Suppose, in fact, that someone proposes the use of a curve, how can we be sure that it does not have some kind of mathematical vulnerability not yet discovered that makes the problem of the logarithm solvable in polynomial times ? **To avoid** the eventuality that some attacker can forge a curve so as to include in it some **mathematical back-doors it is used the principle called nothing up my sleeve**, that is it is introduced a random number, called seed, which is used to generate curve parameters and the generator point, using hash functions. A curve generated by the use of a seed is called veriﬁably random, or randomly veriﬁable

**Quantum Computing: the next (?) revolution in cryptography.**

**Quantum computing** uses quantum-mechanical phenomena, such as **superposition and entanglement.**

We recall that **quantum superposition** is a fundamental principle of quantum mechanics. It states that, much like waves in  classical physics, any two (or more) quantum states   can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct states. Mathematically, it refers to a property of solutions to the Schrödinger equation; since the Schrödinger equation is linear, any linear combination of solutions will also be a solution. An exemplification of this so strange property is the so-called Schrödinger’s cat paradox. **Schrödinger's cat** is a thought experiment proposed by Austrian physicist Erwin Schrödinger in 1935 A cat, a flask of poison, and a radioactive source are placed in a sealed box. If an internal monitor detects radioactivity (i.e. a single atom decaying), the flask is shattered, releasing the poison, which kills the cat. The Copenhagen interpretation of quantum mechanics implies that after a while, the cat is simultaneously alive and dead. Yet, when one looks in the box, one sees the cat either alive or dead not both alive and dead. This poses the question of when exactly quantum superposition ends and reality collapses into one possibility or the other.

**Quantum entanglement** is a still more strange physical phenomenon which occurs when pairs or groups of particles are generated, interact, or share spatial proximity in ways such that the quantum state of each particle cannot be described independently of the state of the other(s), even when the particles are separated by a large distance - instead, a quantum state must be described for the system as a whole. Measurements of physical properties such as position, momentum, spin, and polarization, performed on entangled particles are found to be correlated. **For example, if a pair of particles is generated in such a way that their total spin is known to be zero, and one particle is found to have clockwise spin on a certain axis, the spin of the other particle, measured on the same axis, will be found to be counter-clockwise, as is to be expected due to their entanglement.** However, this behaviour gives rise to seemingly paradoxical effects: any measurement of a property of a particle performs an irreversible collapse on that particle and will change the original quantum state. In the case of entangled particles, such a measurement will be on the entangled system as a whole. Given that the statistics of these measurements cannot be replicated by models in which each particle has its own state independent of the other, it appears that **one particle of an entangled pair "knows" what measurement has been performed on the other, and with what outcome, even though there is no known means for such information to be communicated between the particles, which at the time of measurement may be separated by arbitrarily large distances.**

Such phenomena were the subject of a 1935 paper by Albert Einstein, Boris Podolsky, and Nathan Rosen, and several papers by Erwin Schrödinger shortly thereafter, describing what came to be known as the EPR paradox. **Einstein and others considered such behaviour to be impossible, as it violated the local realist view of causality (Einstein referring to it as "spooky action at a distance")** and argued that the accepted formulation of quantum mechanics must therefore be incomplete. **Later, however, the counterintuitive predictions of quantum mechanics were verified experimentally in tests where the polarization or spin of entangled particles were measured at separate locations, statistically violating Bell's inequality, demonstrating that the classical conception of "local realism" cannot be correct.**

In earlier tests it couldn't be absolutely ruled out that the test result at one point (or which test was being performed) could have been subtly transmitted to the remote point, affecting the outcome at the second location. However so-called "loophole-free" Bell tests have been performed in which the locations were separated such that communications at the speed of light would have taken longer—in one case 10,000 times longer—than the interval between the measurements. Since faster-than-light signaling is impossible according to the special theory of relativity, any doubts about entanglement due to such a loophole have thereby been quashed. **So there is something that is going faster than the light? Or we live in a Multiverse instead of a single Universe? The only answer, for the moment, is that the entanglement is a real phenomenon, that Schrödinger’s cat can be simultaneously dead and alive and that the quantum computing should be possible.**

More in detail a quantum computer is a device that performs quantum computing. Such a computer is different from binary digital electronic computers based on transistors. **Whereas common digital computing requires that the data be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses quantum bits or qubits, which can be in superpositions of states**. A quantum Turing machine is a theoretical model of such a computer and is also known as the universal quantum computer. The field of quantum computing was initiated by the work of Richard Feynman in 1982.As of 2018, the development of actual quantum computers is still in its infancy, but experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits. Both practical and theoretical research continues, and many national governments and military agencies are funding quantum computing research in additional effort to develop quantum computers for civilian, business, trade, environmental and national security purposes, such as cryptanalysis. **A small 72-qubit quantum computer exists and is available for experiments via the IBM Quantum Experience project**

Large-scale quantum computers would theoretically be able to solve certain problems much more quickly than any classical computers that use even the best currently known algorithms, like integer factorization using Shor's algorithm (which is a quantum algorithm) and the simulation of quantum many-body systems. A quantum computers should be able to efficiently solve problems which are not practically feasible on classical computers. A classical computer has a memory made up of bits, where each bit is represented by either a one or a zero. A quantum computer, on the other hand, maintains a sequence of qubits, which can represent a one, a zero, or any quantum superposition of those two qubit states; a pair of qubits can be in any quantum superposition of 4 states, and three qubits in any superposition of 8 states. **In general, a quantum computer with n qubits can be in an arbitrary superposition of up to 2n different states simultaneously.** (This compares to a normal computer that can only be in one of these states at any one time). An example of an implementation of qubits of a quantum computer could start with the use of particles with two spin states: "down" and "up". The advantage is clear: representing the state of an *n*-qubit system on a classical computer would requires the storage of 2n coefficients, while to characterize the state of a classical *n*-bit system it is sufficient to provide the values of then bits.

However when the final state of the qubits is measured, they will only be found in one of the possible configurations they were in before the measurement. Thanks to this property, for some problems, quantum computers offer a polynomial speedup. The most well-known example of this is quantum database search, which can be solved by Grover's algorithm using quadratically fewer queries to the database than that are required by classical algorithms**. An example (and possible) application of this is a password cracker that attempts to guess the password or secret key for an encrypted file or system. This application of quantum computing is, obviously, a major interest of government agencies**. John Preskill has introduced the term quantum supremacy to refer to the hypothetical speedup advantage that a quantum computer would have over a classical computer in a certain field. Google announced in 2017 that it expected to achieve quantum supremacy by the end of the year, and IBM says that the best classical computers will be beaten on some task within about five years. Quantum supremacy has not been achieved yet, and **skeptics like Gil Kalai doubt that it will ever be.** The reason is that if quantum computing will work in a next future, we will have another proof that the existing world is really counterintuitive, much more of what one can imagine thinking to the famous Schrödinger’s cat. In any case, a very promising technology, for the moment, still in the infancy state, that is developing very fast and that could operate a revolution in the cryptography.

**VI LESSONS: THE TECHNOLOGY BLOCKCHAIN APPLIED TO BITCOINS. SYBIL ATTACKS AND YAP ISLAND.**

**Some info about blockchains for bitcoins**

Every user who participates in the Bitcoin network **has a portfolio containing an arbitrary number of cryptographic key pairs**. Public keys, or ”bitcoin addresses”, act as sending or receiving points for all payments. Owning bitcoin implies that **a user can only spend the bitcoins associated with a specific address**. The corresponding private key is used to aﬃx a digital signature to each transaction, making sure that only the user who owns that currency is authorized to pay. The network verifies the signature using the public key**. If the private key is lost, the Bitcoin network will not be able to recognize in any other way the property of the money: the relative sum of money will be unusable by anyone and, therefore, to be considered irremediably lost .**

**The addresses do not contain information about their owners and are generally anonymous**. Addresses in readable form are random sequences of characters and digits **with an average length of 33 characters, always beginning with 1 or 3, of the form 1NAfBQUL4d2N7uu1iKxjwF8dESXTT3AKcq**. **Users can have an arbitrary number of Bitcoin addresses**, and in fact it is possible to generate them at will without any limit as their generation costs little calculation time (equivalent to the generation of a public / private key pair) and does not require any contact with other nodes of the network**. Creating a new key pair for each transaction helps maintain anonymity. Unlike most traditional currencies, Bitcoin does not use a central bank:** it uses a distributed database between network nodes that track transactions, but uses cryptography to manage functional aspects such as generating new currency and the attribution of bitcoin properties. The Bitcoin network allows the anonymous possession and transfer of coins**; the data necessary to use one’s own bitcoins can be saved on one or more personal computers in the form of a digital ”wallet”, or maintained with third parties that perform functions similar to a bank.**

In any case, bitcoins can be transferred over the Internet to anyone with a ”bitcoin address”. **The peer-to-peer structure of the Bitcoin network and the lack of a central body makes it impossible for any government or non-governmental authority to block transfers, sequestration of bitcoins without the possession of their keys or the devaluation due to introduction of new currency.** Unlike legal tender currencies, bitcoins have the characteristic that no one can control their value due to the decentralized nature of the currency creation method. **In Bitcoin the amount of currency in circulation is limited a priori, moreover it is perfectly predictable and therefore known by all its users in advance**. Currency inflation in circulation cannot therefore be used by a central body to redistribute wealth among users.

Transfers are deﬁned as a change of ownership of the currency, and are made without the need for an external body to act as a supervisor between the parties. This **mode of interchange makes it impossible to cancel the transaction and then re-appropriate the coins that have changed ownership.** The Bitcoin client transmits the transaction to its nearest nodes, which verify the authenticity and availability of the funds and in turn relay them back to the nodes to which they are connected. The total number of bitcoins tends asymptotically to the limit of 21 million. The availability of new coins grows like a geometric series every 4 years; in 2013 half of the coins were generated, by the end of 2017 we reached three quarters, so in less than 32 years all the coins will be generated.

**The transactions, digitally signed, are stored in a public register shared by all the nodes and updated with the new transactions, using a scheme called Distributed Ledger Technology**. **The data structure that stores the transaction log is called a blockchain**. The problems that blockchain allows to solve in the context of digital payments, are the **consistency of data in a distributed network**, the definition of a temporal order between events or secure intermediation in trustless environments. **The blockchain is structured as a chained sequence of blocks, each containing a certain number of transactions, in which in each block, with the exception of the first said genesis block, a link to the previous element is contained.** It is therefore a shared database on a peer to peer network that, containing the details of all the transactions carried out on the network, constitutes its historical memory. **The order in which the blocks are concatenated represents a sort of transaction timestamp** that can be used to determine if a given transaction occurred before another.

This idea was used also in the past. At least several hundred years ago, **islanders on Yap in western Micronesia were the precursor to Bitcoin and blockchain technologies.** Based on studies of rock sources and dating of sites on Yap and nearby islands**, before European contact in 1783**, inhabitants of Yap sailed about 400 kilometers to other islands in Micronesia to quarry limestone from caves and rock-shelters. Sea voyagers negotiated with local leaders for access to limestone deposits. Stone carvers went along for the ride and formed stone disks on site. A central hole was cut into each circular chunk of rock so men could run a wooden pole through the opening to hoist the rock. **These weighty pieces of currency, called rai, were transported to Yap on rafts.** Arriving back home, travellers presented newly acquired rai to their fellow community members at a public gathering. Everyone heard which individuals or clan groups took ownership of particular disks.

Each rai was assigned a value based on size, evenness of shape, stone quality and risks taken on the journey. After being inspected and verified by a local chief, rai were displayed at communal spots, such as ritual dancing grounds. **Ownership of a disk could be transferred**, for instance, as a wedding gift, to secure political allies or in exchange for food from residents of nearby islands after a severe storm. **These deals also occurred in front of the whole community. No matter who acquired a rai, it stayed in its original location**. Bitcoin and blockchain work in much the same way. The bitcoin units are transported and securely stored across the public blockchain ledger. **Yap islanders pioneered a public, oral system for securely tracking and exchanging rai. Blockchain does the same by maintaining digital histories and updates about units of cryptocurrency**.

**The mechanism by which new blocks are chained to the blockchain is called mining.** The amount of each transaction is tied to a specific network user by means of some simple instructions of **a non-Turing-complete language called Script. We recall that** a **Turing machine** is a mathematical model of computation that defines an  abstract machine. The Turing machine **was invented in 1936** by Alan Turing.  With this model, Turing introduced the computability theory. Turing completeness is the ability for a system of instructions to simulate a Turing machine. A programming language that is Turing complete is theoretically capable of expressing all tasks accomplishable by computers**. To do this,   the limitations of finite memory are ignored.** This means that the system can end in a loop. In order to avoid this problem, for the bitcoins Satoshi Nakamoto chose a non-complete Turing language.

 In a network where all nodes share constantly changing information, there is the problem of finding a common agreement on what the current state of the system is, this problem is a problem of consensus and the blockchain resolves it in a decentralized way. **In the context of digital payments, these properties guarantee that it is possible to receive or transfer digitally the value, or more generally, an asset, without having to trust the counterparty of the transaction or in a regulatory authority. or in a completely trustless environment.** If we abstract the characteristics related to payment systems, we can use this technology in any context in which we want to make a connected system able to regulate in a secure and independent manner any type of intermediation that may occur within.

**In a distributed network, it is often necessary to certify the creation or modification date of an information so that no one, not even those who have created the information, can alter it.** To implement such a system, it is necessary to publicly make available an infrastructure capable of collecting, processing and renewing time stamps, of digital documents. You can base this type of infrastructure on **a centralized entity called TSS or Timestamping Service** which receives the hash of a document, puts a time stamp on it, generates a new hash starting from the previous one and from the time stamp. his digital signature and sends the signed hash and the timestamp back.

**We recall that a hash is any function  that can be used to map data  of arbitrary size to data of a fixed size.** For instance, we can map a number of 3 cyphers in a smaller number summing the cyphers forming the number. I.e. we map 156 in 1+5+6 =12. 344 in 3+4+4 = 11. The values returned by a hash function are called **hash values or simply hashes.** Hash functions accelerate table or database lookup by detecting duplicated records in a large file. They are also useful in cryptography.  A cryptographic hash function   allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or any equivalent alternatives) by knowing the stored hash value. This is used for assuring integrity of transmitted data. In cryptographic applications we ask, for example, that the hash function has the following properties:

* **resistance to the pre-image**: it is computationally intractable to search for an input string that gives a hash equal to a given hash;
* **resistance to the second pre-image**: it is computationally intractable to search for an input string that gives a hash equal to that of a given string;
* **collision resistance**: it is computationally intractable the search for a pair of input strings that give the same hash

The length of the hash values varies depending on the algorithms used. **The most commonly adopted value is 128 bits, which offers good reliability in a relatively small space**. However, the possibility of using **hashes of larger size SHA (a family of five different cryptographic hash functions developed since 1993 by the National Security Agency (NSA)), for example, can also produce strings of 224, 256, 384 and 512 bits.** The hash functions play an essential role in cryptography: they are useful for verifying the integrity of a message, since the algorithm execution on a text even minimally modified provides a completely different message digest compared to the calculated one on the original text, revealing the attempted change. **The hash functions can also be used to create digital signatures,** as they allow the rapid creation of the signature even for large ﬁles, without requiring long and complex calculations**: it is in fact computationally more convenient to quickly execute a hashing of the text to be signed, and then authenticating only that, thus avoiding the execution of the complex algorithms of asymmetric cryptography on very large amounts of data**. Returning to the blockchain to verify the veracity of the timeline applied to a document **must calculate the hash of the document, calculate a new hash from the latter and the timestamp and compare the result with the message signed by TSS.**

An infrastructure of this type requires that a considerable amount of trust be placed in the certifying authority, which is not always possible. Determining whether a document was created before another implies that it is possible to establish a total order relationship between pairs of documents. In a centralized system complex enough to have multiple TSSs and in which delays or transmission problems may occur, it is possible that this order relation is partial, i.e**. it may not be possible to establish for some documents what was created before. A solution can be to provide a partial order together with a system to solve cases of indecision.** The blockchain represents a decentralized timestamp service, in fact a block is considered more recent than another if it is added after it, for this sort the transitive property holds and furthermore, assuming that the sequence of blocks not present bifurcations, this order is total. **As a result, a transaction is considered more recent than another if it is contained in a more recent block. In case the two transactions were contained in the same block, they are sorted according to the order in which they appear inside the block.**

How to find the agreement? If we think of a group of individuals who must agree on something, **an idea to solve the problem is to proceed to a simple vote and let the majority decide**. This approach can be valid if they vote, at the most, only those entitled, but in a digital system, where it is possible to create fictitious identities that act as voters, this mechanism could does not work. If it is possible to create a sufficient number of fake identities to subvert the outcome of the vote, then a system to reach consensus by quorum could be controlled at will, this situation is known as Sybil Attack**. A Sybil attack can work if, within a voting system, an attacker can create an arbitrary number of pseudonyms without any particular burden.** Therefore, not being able to prevent the creation of more voters’ identity, **one of the solutions consists in requiring that the voting operation has a cost that makes it uneconomical for an attacker to create aliases** with which to subvert the outcome of the vote. vote. This approach is based on the proof-of-work concept, which is an operation that is expensive to calculate, but simple to verify.

**VII LESSON: HOW IS POSSIBLE TO AVOID THE DOUBLE SPENDING? HOW DOES THE BLOCKCHAIN TECHNOLOGY WORK IN THE BITCOIN WORLD?**

**Suppose we want to implement a simple election based on proof-of-work, a vote will be a string that expresses the voter’s preference**. The result of the vote will be determined by the majority of the votes collected in a given time frame and each participant will be able to vote as often as he likes, **the only condition that we will impose is that the hash of a valid vote begins with a particular string, for example a single zero**. **To generate a valid vote we will have to create a string in which the name of the preference is expressed, plus a nonce, made up for example by the number of the attempt in progress and by a random value.** In this way the last part of the voting string changes until its hash does not respect the established criterion.

Furthermore. By protecting the voting operation with a computational cost, we have somehow discouraged a determined attacker to flood the digital urn with thousands or millions of votes, making it uneconomical to influence the system with a Sybil attack, or to cause disruptions due to high traffic generated. It is not a coincidence that HashCash, one of the first applications of the proof-of-work concept, was aimed at containing the problem of spam and DoS attacks. **An alternative way to reach the majority to award the vote could be to ﬁx a rather high difficulty and count only the first valid vote found. This situation is equivalent to organizing a sort of competition whose winner will receive as a prize the right to express the only valid vote.** To get an idea of the difficulty of requesting such a competition, requesting a digest that starts with 6 zeros would require more than 700,000,000 attempts to calculate a valid vote

**It may seem a bit extreme to handle the problem of consensus, but it is not unlike what is being done by the mines to link a new block to the blockchain**. Each miner generates a new block including new transactions in it and calculates the proof-of-work, as soon as it is able to calculate a valid hash it concatenates blocking to the blockchain. For each block successfully linked to the miner, a certain amount of new bitcoins is paid to compensate for the computational eﬀort sustained. Because a system of this type functions it is necessary that the output of the selected hash function is completely different every time we modify the input. **Therefore generating a valid vote is not just a diﬃcult problem, but it is also something very similar to trying to win a lottery, since every attempt returns a completely different result from the previous one.** The probability of finding a digest that starts with a number n of zeros is equivalent to determining the probability of a partial collision with the string consisting of n zeros. Each character of a digest generated by SHA-256 is a hexadecimal number, that is, it can assume 16 possible values, so the probability of a collision with a specific string is the inverse of the number of possible hash of length n, that is (1/16) to the power n.

Another problem to be faced is that related to the **limitations given by Theorem CAP**, i.e. that a distributed system can at most guarantee two of the three properties: consistency, availability and partition tolerance. Obviously**, since availability and partition tolerance are indispensable**, the property to be weakened is the one relating to consistency. Consider the three levels of consistency that data can have in a distributed system:

* **no consistency**: the system does not need any consistency and, not having problems in data synchronization, it allows to have a service availability and a tolerance to the maximum partitions;
* **strong consistency**: the system requires that at all times all the individual nodes see exactly the same data, so if a node were to disconnect, the system would be unable to continue its operation, at least until the node reconnects;
* **weak consistency:** the system can continue to operate in the case of partitioning the network, allowing data to be misaligned, at least temporarily.

**The most interesting consistency category** for a distributed fault tolerant system **is the weak one**, so it is essential to establish a policy that will allow you to resolve any conflicts once the partitioning is over, re-aligning the data between all the nodes**. The blockchain guarantees a weak consistency model of the data in which the availability of the transaction log is guaranteed to all connected nodes**, with some peculiarities:

**- the records of transactions** held by some nodes **may not be synchronized**, at least temporarily;

- **the system must be able to converge** on a global ordering of all transactions;

 - **the system must be able to resolve conflicts** in the data in a predictable way;

- **the system must prevent a bitcoin from being spent more than once**

 - **the system must be protected against Sybil attacks.**

**The blockchain has been designed to cryptographically ensure the integrity of the transaction log**, for this purpose the entire infrastructure is built as a communication system based on digital signature with the following characteristics:

 **- information** regarding a single transaction **cannot be corrupted** without leaving a trace;

- a **transaction**, once finalized, **cannot be repudiated** by the parties;

 **- each transaction is attributable** to the counterparties involved.

**The digital signature serves both to constrain each transaction to its owner**, who is the only one who can dispose of the funds contained in it, and **to ensure that the funds transferred from a transaction are paid only to the legitimate recipient**, who will become the new master. Once a transaction has been accepted by the system, the only way to alter its data is to modify the block in which it appears, in addition to all the blocks that have been concatenated to it later, which is computationally impractical. **The algorithm used for the digital signature is based on the arithmetic of elliptic curves** and its strength depends mainly on the type of elliptical curve that is chosen, some curves in fact have some mathematical vulnerabilities and therefore their use is not recommended in cryptography.

**The particular elliptical curve used and made popular by Bitcoin is called secp256k1 and, unlike the standard curves recommended by NIST, is a curve whose parameters and constants have been chosen in a predictable and well documented manner**. For this reason it is thought to be rather unlikely that its creator has deliberately introduced you some mathematical backdoors. In addition, it is a curve that lends itself particularly to efficient calculations on a computer, allowing an increase in performance up to 30 % compared to other curves if the implementation is quite optimized. In addition to using the digital signature algorithm, the blockchain uses different hash algorithms to ensure the integrity of the transactions contained in each block and the block itself, to achieve consent by proof-of-work and to generate valid bitcoin addresses.

A **Public Key Infrastructure or PKI** is an infrastructure composed of both hardware and software tools as well as **procedures and protocols used to ensure that the electronic transfer of information between a set of subjects can be carried out safely**. When there is a need to send confidential data between different counterparts in distributed and therefore potentially insecure environments, three components are needed:

 - **authentication** of participants in the system;

 - **encryption** of messages;

- the **non-repudiation** of messages;

The authentication of the participants serves to validate the identity of those who send and receive messages on the infrastructure, be they individuals, websites or software agents, ensuring their identity. This component ensures that on the PKI everyone is who he claims to be.

The encryption of the messages ensures the confidentiality of the data sent, if an unauthorized person were to intercept the message in fact could not decrypt the content if the encryption algorithm used is quite robust. This component ensures that data is readable only by those who are effectively authorized to do so. The non-repudiation of messages is the assurance that the exchanged messages cannot be altered during their transfer and also guarantees the authenticity of the sender’s identity. This component ensures both the paternity and the non-alterability of messages sent over the network**. The network of Bitcoin nodes joined to the blockchain can be considered as a PKI in which, in order to guarantee to every node the possibility to control the transaction register, the encryption of the messages is not implemented.**

**Bitcoin is born to be free from any form of control or constraint**, therefore it is entirely open source. This guarantees all interested parties the possibility of verifying the code or protocol, reporting problems and proposing improvements. A decentralized infrastructure removes the need to have bodies that certify and finalize transactions, with obvious positive repercussions of practical order:

**- the single point of failure of the system is eliminated** and the load is distributed on all the nodes making the system more robust and resilient;

- **eliminates the risk that a centralized entity**, responsible for the validation of transactions or the issuance of money, betrays this trust due to incompetence or dishonesty;

- **the brokerage costs for operations are reduced**, because it is no longer necessary to maintain a separate infrastructure to validate and make transactions effective;

 - **it is not technically possible to confiscate** or steal funds from a user unless he knows his private key.

**Bitcoin is a push payment system**, i.e. **it does not require anyone who sells, accesses or stores information about their customers and their transactions.** **In a pull system, instead, this information accumulates in the databases of e-commerce sites and represents sensitive objectives that can be violated**, compromising the security of the data contained, such as credit card credentials or personal information of customers. In Bitcoin all transactions are referred to pseudonyms, so it is not immediate to establish within the system, a link between a real physical identity and a set of transactions and vice versa. **It is not necessary to place trust in the human factor**, which is generally the weak link in a security-oriented structure, in fact there is little to do with firewalls, cryptographic protocols and security devices to stop an individual or an organization that, by acting dishonestly, tries to take advantage of the system it should control. On the contrary, by its nature, **Bitcoin presents some disadvantages that are diﬃcult to solve, for example the funds can only be used by means of a private cryptographic key; if this were to be lost, the related funds would also be lost without any possibility of recovery**.

Since this is a system without authorities and guarantors and financial institutions that provide services to the public**, there is no assistance service to refer to in case of problems such as loss or theft of your wallet**. **Bitcoin has attracted the attention of financial speculators** and this in the absence of a central authority that regulates the operating parameters **has led to an extreme volatility of its value.** Bitcoin is a peer-to-peer electronic money system that ensures secure brokerage and value transfer in trustless environments. **Unlike traditional payment systems, it allows counterparties to perform direct operations,** delegating their validation and implementation to the entire network of participating nodes.

Let’s see what happens when two users decide to make a transaction, let’s assume that **Bob wants to transfer 1 Bitcoin to Alice:**

 - **Bob’s wallet creates a new transaction** and sends it to the network;

 - **the nodes receive the transaction** and after having validated it they send it to their neighbours;

- **the transaction arrives at a miner** that verifies its correctness;

- **the miner inserts it, together with the other transactions to be confirmed, of which he has knowledge, in a block;**

 - **the miner calculates the proof-of-work of the block** and adds it to the Blockchain propagating it on the network;

 - **the nodes receive the new block**, verify it and send it to their neighbours;

 - **the block arrives at Bob and Alice**, confirming the success of the operation;

The transaction sent by Bob goes a long way in the peer to peer network, is propagated until it reaches the miner that will succeed in inserting it into the new block of the Blockchain and from there, inside a new block, reaches all the nodes of the network, is propagated again throughout the network, this time as a confirmed transaction, i.e. included in the Blockchain, until it reaches the two nodes representing Alice and Bob. **Despite all the steps necessary for validation and implementation, the transfer of value takes place directly from those who pay to whom receives, being Bitcoin a push payment system. The time needed to concatenate a new block to the Blockchain is about 10 minutes which, considering the propagation times of the messages within the network to be negligible, represents the time necessary for each transaction to be verified and included in the Blockchain.**

The Blockchain is a data structure that contains the database of completed transactions, stored within concatenated blocks in a single linked structure. This data structure is shared by all the nodes of the network and is continually updated by concatenating each new block to the last one. To maintain the relationship with the previous element in the chain, **each block stores the blockhash of its own father, this value is calculated as a hash of the block and therefore uniquely identifies it.** The unique back link for which each block has only one parent **but may have, at least temporarily, more than one child, that is, there may be more blocks that refer to him and that thus they generate a fork.** Generally this inconsistency **occurs when two or more blocks are discovered and propagated almost simultaneously**, but once the bifurcation is resolved with appropriate mechanisms, only one of the blocks will be confirmed in the Blockchain remaining an only child.

**VIII LESSON: THE MINERS. THE NEW TECHNOLOGIES APPLIED IN MINING.**

The blocks are deposited on one another as geological sediments and the sequence in which they are linked is a temporal order for the transactions contained therein. Moreover, like the geological sediments**, the most ancient blocks are even more stable because their value influences the blockhashs of all the blocks that follow it in the chain so to modify a block it is necessary to modify also the whole chain that descends from it so that it is composed of valid blocks.** Mining is the process by which new bitcoins are produced but above all the mechanism by which consensus is reached on the status of transactions within the network. The miners, that is the nodes specialized in this operation, are responsible for keeping the transaction log updated. In the intent of the protocol the task of the miners is essential for the proper functioning of Bitcoin and represents a service of public utility, incentivized by the perspective of individual gain.

The difficulty of the work required by the miners to generate new blocks is designed to automatically adapt to maintain the constant frequency of the constant Blockchain. To allow us to**, every 2016 blocks the network resets the proof of work difficulty based on the speed with which the blocks were added** and therefore based on the computing power of the network. Since a transaction ca not be included in more than one block and since the blocks are added individually to the last element of the Blockchain, **a real race is going on between the miners, said mining competition, to be able to calculate a new block before the others.**

**The competition, also due to the increase in bitcoin prices, has increased dramatically in recent years and this has forced the miners to increase its computing power to stay in the game and be competitive in the race to calculate the new blocks.** From this upward game there arose a vicious circle whereby the computational power of the miners progressively increased, but this increase was matched by an increase in proof-of-work difficulty. This means a incredible waste of energy. It is estimated that **the current global power consumption** for the servers that run bitcoin’s software is a minimum of 2.55 gigawatts, **almost the same as Ireland**. Google, by comparison, used one fifth of this energy in 2015. What’s more, bitcoin “miners” consume about five times more power than they did last year, and orders of magnitude more than just a few years ago, and there are no signs of a slowdown.

The hardware used for mining operations has undergone profound changes over the years, over the years it has **gone from solitary miners, sometimes simple PCs possibly enhanced by rudimentary gpu computing tools, to real clusters, called mining pools, formats from devices specialized in the calculation of large quantities of hashes**. These specialized structures, in order to function, must sustain a considerable number of costs:

 - **hardware acquisition and maintenance**,

 - **electricity supply**

- **connectivity**

- the **costs inherent the physical structures where the hardware is to be maintained**.

More in detail , till few year ago it was used the **mining rig** that was a computer system used for mining bitcoins.  The rig might be a dedicated miner where it was procured, built and operated specifically for mining or it could otherwise be a computer that fills other needs, such as performing as a gaming system, and is used to mine only on a part-time basis. Note that **GPU mining is not very profitable (if at all)** anymore, and even if you have free electricity, GPU (Graphic processing Unit) rigs **will likely never pay for themselves** at this point. We recall that **a GPU is a specialized electronic circuit  designed to rapidly manipulate and alter memory   to accelerate the creation of images**   in a frame buffer  intended for output to a display device. Modern GPUs are very efficient at manipulating computer graphics and image processing.  The term GPU was first used in at least 1980s, it was popularized by Nvidia  in 1999 and used nowadays by Commercial Banks to create different scenario of investments.

The GPU mining was replaced by the **Application-Specific Integrated Circuit** **(ASIC)** that is an **integrated circuit** customized for this particular use i.e. to be a high-efficiency Bitcoin miner. As feature sizes have shrunk and design tools improved over the years, the maximum complexity (and hence functionality) possible in an ASIC has grown from 5,000  logic gates to over 100 **million. Modern ASICs applied to bitcoins often include entire microprocessors, memory blocks** including ROM, RAM, EEPOM, flash memory, etc. Also the ASIC approach is not more profitable and nowadays the **last frontier are FPGA (Field-programmable gate arrays)** that are the modern-day technology for building a breadboard  or prototype from standard parts; programmable logic blocks and programmable interconnects allow the same FPGA to be used in many different applications.

**The FPGA configuration is generally specified using a hardware description similar to that used for an ASIC.** FPGAs contain an array of programmable logic blocks , and a hierarchy of reconfigurable interconnects that allow the blocks to be "wired together", like many logic gates that can be inter-wired in different configurations.  Logic blocks can be configured to perform complex combinational functions, or merely simple logic gates  like  AND and XOR. In most FPGAs, as in ASICs, logic blocks also include memory, which may be simple flip-flops or more complete blocks of memory. **Many FPGAs can be reprogrammed to implement different logic functions, allowing flexible reconfigurable computing as performed in computer software.**

**To incentivize this activity to the miners**, it is allowed to **attribute, for each block successfully calculated, a reward** that is claimed by inserting on the top of the new block a transaction called generation or coinbase, which contains the height of the generated block, whose value is currently 12.5 bitcoins. **An additional incentive for mining activity is given by transaction fees**, voluntary donations included in new transactions to incentivize the miners to take charge of them as soon as possible. **Paying a transaction fee is optional.** Miners can choose which transactions to process, and they are incentivised to prioritize those that pay higher fees. Because the size of mined blocks is capped by the network, miners choose transactions based on the fee paid relative to their storage size, not the absolute amount of money paid as a fee**. Thus, fees are generally measured in satoshi per byte**, or sat/b (Each bitcoin (1 BTC) can have a fractional part of up to 8 digits so 1 bitcoin can be divided into 100 000 000 units. Each of these bitcoin units (0.00000001 BTC) is called a satoshi. A satoshi is the smallest unit in a bitcoin). The size of transactions is dependent on the number of inputs used to create the transaction, and the number of outputs.

**The bitcoin amount guaranteed by a generation transaction is designed to decrease over time**, the more precisely its value is halved every 210000 new blocks, so you can estimate the amount of money produced with the geometric series:

∑210000×(50)(1/2)n= 21000×50×2 = 21000000 Bitcoins

In order to implement safe value exchanges, it is necessary that each node is in agreement on the status of the Blockchain and therefore on the register of the transactions carried out, in order to reach this agreement in the absence of a central body it is necessary that the consensus implicitly emerges as a consequence information held by the individual nodes. **We therefore speak of an emerging consensus, that is, the consensus is a product of the asynchronous interaction of thousands of independent nodes** that, in order to cooperate, follow the same rules.

**Bitcoin was designed not to need a central authority and the bitcoin network is considered to be decentralized**. However, researchers have pointed out a visible ”trend towards centralization” by the means of miners joining large mining pools to minimise the variance of their income. According to researchers, other parts of the ecosystem are also ”controlled by a small set of entities”, notably online wallets and simplified payment verification (SPV) clients. **Because transactions on the network are confirmed by miners, decentralization of the network requires that no single miner or mining pool obtains 51% of the hashing power,** which would allow them to double-spend coins, prevent certain transactions from being verified and prevent other miners from earning income. As of 2013 just six mining pools controlled 75% of overall bitcoin hashing power. In 2014 mining pool Ghash obtained 51% hashing power which raised significant controversies about the safety of the network. The pool has voluntarily capped their hashing power at 39.99% and requested other pools to act responsibly for the beneﬁt of the whole network.

Within Bitcoin, achieving consensus derives from four operations that, potentially, each node carries out:

 - **verification and propagation of every single transaction**;

 - **independent aggregation of transactions into new blocks**, on which the proof-of-work is calculated;

 -**independent verification of each new block and inclusion in the local copy of the Blockchain**;

- **selection**, in case of fork, **of the longest chain**.

Each node provides for the validation and then the propagation of transactions, in this way the spread of malformed transactions is limited and maximum transparency is guaranteed with respect to the operations carried out in the system. Similarly**, the nodes are responsible for verifying and disseminating new blocks**, so that if most of the nodes work according to the rules, we can expect the new blocks to be propagated in the network and then linked to the new Blockchain, only if they have been produced according to the rules. **However this does not protect the Blockchain from temporary inconsistencies, in fact it can happen that two blocks are calculated and propagated almost simultaneously**.

As a result, a part of the network could take the Blockchain as correct, which includes the first block and another part could take the one that includes the second as correct. Taking again the terminology already used for the CAP theorem**, the system guarantees a weak consistency of data, that is, it admits that there are temporary inconsistencies that are resolved in a predictable manner**. **The criterion for resolving this type of conflict uses the amount of work spent on proof of work as a unit of measurement of the validity of a chain.** If a node receives two versions of the opposing Blockchain, it immediately accepts and propagates the longer one, that is, the one that required the most work to be created. All transactions that were contained in the shortest chain and that are not included in the longest chain are put back into play, ie they are considered unconfirmed transactions and therefore can and should be included in a new block from someone of the miners.

In practice, **the bifurcations of the Blockchain are identified and then resolved rather quickly**, this prevents chaotic situations in which there are more alternative chains, but **does not protect us from the possibility that a generic block on the main chain is discarded if another long chain is found that does not contain it**. The only assumption you can make is that the longest chain of blocks that originates in a block within the Blockchain is more diﬃcult than it can be discarded or altered due to the amount of work that would be needed. Moreover, while an attacker is intent on recalculating the proof of work of the block he intends to modify, more than his successors, the Blockchain continues to lengthen by the miners.

 Based on what has been said up to now we summarize the properties of the Blockchain:

- **the individual transactions** are digitally signed, they **are not repudiable** and their integrity is cryptographically guaranteed;

- once the transactions have been created, **they are sent to all nodes** of the p2p (peer to peer) network;

- **each block contains at least one transaction** and each transaction present in a block must be valid;

- **each block contains a link to its parent block**;

- **each node of the network can generate a valid block**, exhibiting a correct proof-of-work;

 **- the difficulty of tampering with a block increases with the lengthening of the chain that originates in it**;

 - **if a bifurcation is detected, the network itself decides in a predictable way**;

- **the inclusion of a transaction in a block acts as a confirmation** of its execution.

**A hard fork is a rule change such that the software validating according to the old rules will see the blocks produced according to the new rules as invalid.** In case of a hard fork, all nodes meant to work in accordance with the new rules need to upgrade their software. **If one group of nodes continues to use the old software while the other nodes use the new software, a split can occur**. For example, Ethereum has hard-forked. In June 2016, users exploited a vulnerability in the DAO code to enable them to siphon oﬀ one third of The DAO’s funds to a subsidiary account. On 20 July 2016 01:20:40 PM +UTC at Block 1920000, the Ethereum community decided to hard-fork the Ethereum blockchain to restore virtually all funds to the original contract. This was controversial, and led to a fork in Ethereum, where the original unforked blockchain was maintained as Ethereum Classic, thus breaking Ethereum into two separate active blockchains, each with its own cryptocurrency.

**A wallet stores the information necessary to transact bitcoins**. While wallets are often described as a place to hold or store bitcoins, due to the nature of the system, bitcoins are inseparable from the blockchain transaction ledger. A better way to describe a wallet is something that ”stores the digital credentials for your bitcoin holdings” and allows one to access (and spend) them. There are three modes which wallets can operate in. They have an inverse relationship with regards to trustlessness and computational requirements. **Full clients verify transactions directly by downloading a full copy of the blockchain** (almost 200 GB). They are the most secure and reliable way of using the network, as trust in external parties is not required. Full clients check the validity of mined blocks, preventing them from transacting on a chain that breaks or alters network rules. Because of its size and complexity, downloading and verifying the entire blockchain is not suitable for all computing devices.

**Lightweight clients consult full clients to send and receive transactions without requiring a local copy of the entire blockchain**. This makes lightweight clients much faster to set up and allows them to be used on low-power, low-bandwidth devices such as smartphones. **When using a lightweight wallet, however, the user must trust the server to a certain degree**, as it can report faulty values back to the user. Lightweight clients follow the longest blockchain and do not ensure it is valid, requiring trust in miners. **Third-party internet services called online wallets offer similar functionality but may be easier to use**. In this case, credentials to access funds are stored with the online wallet provider rather than on the user’s hardware. **As a result, the user must have complete trust in the wallet provider.** A malicious provider or a breach in server security may cause entrusted bitcoins to be stolen. An example of such a security breach occurred with Mt. Gox in 2011. This has led to the often-repeated meme ”**Not your keys, not your bitcoin**”.

**IX LESSON: IS BITCOIN A CURRENCY?**

**At the beginning of 2014, Mt Gox, a bitcoin exchange based in Japan, was the largest bitcoin exchange in the world, handling over 70% of all bitcoin transactions worldwide. By the end of February of that year, it was bankrupt.** **The victim of a massive hack, Mt. Gox lost about 740,000 bitcoins** (6% of all bitcoin in existence at the time), valued at the equivalent of $460 million at the time. An additional $27 million was missing from the company’s bank accounts. **Although 200,000 bitcoins were eventually recovered, the remaining 650,000 have never been recovered**. The blocks in the blockchain were originally limited to 32 megabyte in size. The block size limit of one megabyte was introduced by Satoshi Nakamoto in 2010, as an anti-spam measure. Eventually the block size limit of one megabyte created problems for transaction processing, such as increasing transaction fees and delayed processing of transactions that cannot be ﬁt into a block. On 24 August 2017 (at block 481,824), Segregated Witness (SegWit) went live, **introducing a new transaction format and the block capacity may be 1.25 megabytes.**

**Is Bitcoin a currency?**

By money we mean everything that is used as a means of payment and intermediary of exchanges and that performs functions of:

- **unit of measurement of the value of a good or service**;

-**instrument of exchange in the sale of goods and services**;

 - **fund and accumulation of value**.

**Most of the money in circulation nowadays is made up of ﬁat coins or legal currencies, or coins that do not have a direct or indirect intrinsic value**, as they are not tied to a consideration as well as gold could have been in the past or silver. Before the advent of the ﬁat coins, that is until relatively recently, the currencies of the western states were linked to the national gold reserves, this because it is:

 - **there was a need to correspond to each individual currency a material guarantee of its value**;

- **gold has excellent resistance to corrosion** and can be split;

**- the rarity of gold makes it possible to control production** without risking inﬂation.

**Legal coins are valid and have a certain value by decree**, or because some type of sovereign authority, typically a national state, acts as if the currency had a certain value. The characteristics of a legal currency are

- **its stability is guaranteed by the control over the issue carried out by a Central Bank**, necessary to manage the supply and the availability of money;

- **recognition as a means of payment is guaranteed by law**;

- **the purchasing power of the currency on the basis of the two previous points is only relevant in relation to the goods, services and ﬁnancial products available in the country** or countries in which this currency circulates.

In this context, **the value of a currency is linked to trust in the State that guarantees its validity** as a means of payment, so that its performance can be aﬀected by strategic or economic choices such as energy exposure, industrial policy or military security of national borders. Extending the concept we can say that if a group of people decides to issue, use or accept a good as payment, that asset automatically acquires value and becomes a currency, since it is a means of exchange within the community. and can be used as accumulation and value measurement unit.

**Therefore, within a common, any good can, in principle, assume the role of money.** During the Second World War, for example, a certain number of cigarettes were supplied, together with the daily ration of food, inside the military prison camps. It was therefore normal that non-smoker prisoners, or any surplus on the daily ration, would give their cigarettes to smokers in exchange for other goods or services. The practice was so widespread that cigarettes went from being a simple good of comfort to cover the function of real money circulating inside, subject in all respects to internal or external events that determined shortage or abundance. **Physical currency as we know it, money circulating in the form of banknotes and coins, has become an integral part of our daily life, so much so that even in a technologically advanced and extremely connected society no individual can to do without**. However, despite its intrinsic necessity, money presents several practical disadvantages for the user:

- to be spent, **it must be physically transported**;

 - **it is not very hygienic**;

- **it is cumbersome**;

 -**it can be stolen or lost**.

While on the one hand, **digital payment systems have reduced the amount of money circulating in our society**, even if they cannot completely eliminate it, on the other hand they have also **opened a series of problems** still open since point of view of privacy. **An observer who was able to consult the payment transactions that we carry out could completely reconstruct our habits, our lifestyle and much more without too much eﬀort**, by contrast, money intended as physical money, is practically untraceable. The term payment systems means: a set of tools and procedures aimed at reducing the material movements of money from one subject to another, in order to regulate the economic transactions established. This translates into the possibility of paying a pecuniary obligation, such as the payment of a good or a service, by means of instruments such as checks and bank transfers, which use bank money or credits available in bank deposits.

**Technological development has required payment systems to adapt to new conditions of use, such as the online payment market**, whereby banks and ﬁnancial institutions that manage payment systems have had to evolve their tools together. In the world of credit card payments, over the years, various standards have been proposed to make transactions secure, among these one of the most well known is **Secure Electronic Transaction**, a speciﬁc proposal by the main operators in the sector in 1996 In its full version it was a rather complex system that involved the eﬀort of various components to ensure the security of every single transaction. **The SET procedure was abandoned in favour of the most recent 3-D Secure** which, although receiving severe criticism, has now become a standard whose main implementations are Veriﬁed by Visa and Mastercard Securecode. **Credit card payments are the most used and accepted mostly online, their operating scheme is called ”pull” and is based on the complete intermediation of the credit institutions of the counterparties.** The cardholder provides, through his credit institution, said Issuer, the authorization to withdraw the amount due from his account, to the creditor institution, called Acquirer.

**It is therefore necessary that the cardholder puts trust in the entire payment chain**, or at least on the assurance that his credit institution re-establishes any fraud and misappropriation by a fraudulent creditor or a generic malicious agent. **Cash instead acts as a push payment system, or to make a payment you must physically withdraw from your wallet the desired amount and then you must deliver it to the other party**. There is no need to guarantee access to your wallet to a seller or a certiﬁed authority to make a payment. Digital currency means a digitized exchange medium, not necessarily linked to any physical currency, that can be exchanged with goods or services within connected communities, such as a social network or an online game. **Some, called virtual, can only be exchanged within a community and are generally under the direct control of its developers and administrators. An example is the Amazon Coin that function as a gift card and can be used to buy products internally at Amazon, but cannot be converted into cash**. In order to be able to use a digital currency within payment systems, it is necessary that it be exchanged for real-world goods, services and currencies, but this feature, even if necessary, would not be suﬃcient on its own.

It is possible to deﬁne a set of **characteristics that an ideal digital currency system** should have:

 - **independence**, the security of digital credits must not be dependent on any physical location,

 - **the quantities must be able to be transferred through a computer network**;

 - **security**, credits cannot be duplicated and reused;

- **no traceability**, the user’s privacy must be protected, nobody must be able to identify a relationship between the user and what he / she bought;

- **oﬄine payments must be possible** when a user makes a payment, the protocol between the user and the seller is performed oﬀ-line, i.e. the store does not need to be connected to process the payment;

- **transferability,** credits must be able to be transferred to other users;

- **divisibility**, a quantity of digital money must be divisible into smaller units. It is interesting to note how, together with characteristics related to the good functioning of the currency, such as security, the privacy of users also plays a prominent role, in this direction digital coins that use cryptography are moving.

**To meet the ever-growing demand for security and privacy, the world of digital currencies is increasingly closer to that of cryptography**. Cryptographic or cryptographic digital coins use cryptographic functions to guarantee the security of transactions and possibly to issue new credit. **One of the earliest examples in this context was e-cash, a completely anonymous centralized electronic money system, which used RSA to make the blind digital token signature, which were issued and converted by a regular bank.** Theoretically a digital currency, just like any ﬁle, can be copied more than once and therefore, a system is needed that prevents a user from spending the same coin, or a copy thereof, more than once, this anomaly is known as a double expense problem**. In a system such as e-cash transaction controls are delegated to the bank that issues tokens, which, for greater security, are destroyed by the bank once converted into money by a user. The result is a centralization of responsibilities, and information, with obvious risks to the security and integrity of the system, as well as to the privacy of users, both due to external and internal agents.**

**Any exchange of goods and services requires some form of accounting** and, as we have seen, modern payment systems are mostly centralized. This means that banks or credit institutions check and arrange the transfer of money from one user to another, consulting and updating the information contained in their registers. In the absence of a centralized entity that tracks the status of accounts of users and guarantees the regularity of exchanges, it is necessary that all users can consult the transaction log. **If everyone knows the history of a token, everyone can determine if it is expendable by a particular user, because everyone knows if the user is still owner or has already spent it**. **The absence of a centralized system requires the use of some kind of Distributed Ledger Technology or, to distribute, update and make public the transaction register.** Two examples in this sense are bitgolds and b-money, which, however, although decisive in the development of modern decentralized cryptocurrency, do not provide a mechanism able to put all nodes in agreement on the transaction log, in other words do not propose a solution eﬀective to the problem of consensum, unlike Bitcoin.

**The Bitcoin system is based solely on mathematical and algorithmic principles.** As one can imagine, at its beginnings, bitcoin payments were mainly accepted by private individuals, small retailers and sites of exchange and e-commerce sometimes of dubious fame, but recently **large world brands have begun to introduce bitcoin as a form of payment**, including Microsoft, Dell and Overstock. In addition to being strongly security oriented, Bitcoin still remains the most widely used crypto-money in the world today, despite the not very benevolent attention of ﬁnancial institutions, governments and hackers and despite the competition of alternative digital coins born in its wake, the so-called altcoins. According to a research produced by Cambridge University**, there were between 2.9 million and 5.8 million unique users using a cryptocurrency wallet, as of 2017, most of them using bitcoin**. The number of users has grown signiﬁcantly since 2013, when there were 300,000 to 1.3 million users. In 2015, the number of merchants accepting bitcoin exceeded 100,000. Instead of 2-3% typically imposed by credit card processors, merchants accepting bitcoins often pay fees under 2%, down to 0%. **Firms that accepted payments in bitcoin as of December 2014 included PayPal, Microsoft, Dell, and Newegg**. In 2017 bitcoin’s acceptance among major online retailers included three out of the top 500 online merchants, down from ﬁve in 2016. Reasons for this fall include high transaction fees due to bitcoin’s scalability issues, long transaction times and a rise in value making consumers unwilling to spend it.

**In November 2017 PwC accepted bitcoin at its Hong Kong oﬃce in exchange for providing advisory services to local companies who are specialists in blockchain technology and cryptocurrencies**, the ﬁrst time any Big Four accounting ﬁrm (The Big Four are the four largest professional services networks in the world, oﬀering audit, assurance services, taxation, management consulting, advisory, actuarial, corporate ﬁnance and legal services, they are Ernst Young, DeLoitte, KPMG, PwC) accepted the cryptocurrency as payment. **In a 2013 report, Bank of America Merrill Lynch stated that ”we believe bitcoin can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money-transfer providers.”** In June 2014, the ﬁrst bank that converts deposits in currencies instantly to bitcoin without any fees was opened in Boston. Plans were announced to include a bitcoin futures option on the Chicago Mercantile Exchange in 2017.Trading in bitcoin futures was announced to begin on 10 December 2017 The success of the bitcoin comes also rom the fat that, from the end user’s point of view, the elements necessary to use Bitcoin are:

- **a pair of public / private keys**;

 -**an address to receive coins**;

 - **a wallet software**;

 - **an internet connection**.

Obviously it is necessary to have some cares using bitcoin. Note the parameters of the curve used it is possible to generate a pair of keys that will be stored in the wallet. **It is important that the private key remains secret**, as it serves to have its own bitcoins, instead the public key can be made public and is used to generate its own bitcoin address using the RIPEMD1605 hash function. The wallet is used to manage the key pair, to carry out transactions and to obtain useful data from the blockchain, for example the balance of its expendable bitcoins. **Contrary to what the name may suggest, the wallet does not physically contain the bitcoins of the user, but rather contains the key needed to spend them and the address to which they can be received. Each user can use his own bitcoins exclusively through his private key, so if this key is lost the credits associated with it will no longer be usable. In a sense, the price to be paid for the independence of the whole system is that each individual participant is solely responsible for their credits**.

**X LESSON: IS THE PRESENT VALUE OF THE BITCOIN FAIR? WHAT ABOUT THE FUTURE OF THE BITCOIN?**

**If you want to acquire or vice versa to convert your bitcoins into real money, there are so-called Exchange sites** whose operation is similar to that of a foreign exchange institution. A user deposits a sum in the currency he wishes to change and with that sum he exchanges in other currencies with other users, until he decides to withdraw the amounts. The exchange works by sending orders to the system such as: buy / sell a certain amount of currency at a certain exchange rate in response to which compatible requests will be sought by matching supply and demand.As already written, **unlike regular credit cards, Bitcoin is a push payment system, meaning a bitcoin can be spent with the same logic as cash**. If you intend to make a payment, a transaction is created and a certain amount is transferred to a beneﬁciary. **There is no need to allow third parties to access their account or to release personal information such as their own economic availability or data relating to their identity.**

**The value of a currency is also linked to its diﬀusion, that is to say how large its user base is and how high its level of acceptance is with those who provide services or sell goods. During its ﬁrst years of life the value of a bitcoin was almost purely nominal,** the ﬁrst recorded transaction, as already mentioned, dates back to 2010 and was the payment of two pizzas per 10000 bitcoins. A few months later **the ﬁrst and only attack against Bitcoin was carried out until now, exploiting a vulnerability on transaction veriﬁcation, some hackers managed to create 184 billion bitcoins in one transaction, in just a few hours the vulnerability was found and corrected and the fraudulent bitcoins destroyed.** Among the causes of the performance of the value of Bitcoin, **there is probably a shift from a simple medium of exchange to an object of ﬁnancial speculation. A further element that inﬂuences the value of money is the way it is issued, in fact, in Bitcoin there is no central authority that in case of need provides for the expansion of the monetary base.** The new bitcoins are put into circulation as a reward for the nodes that are concerned with updating and maintaining the blockchain, as a reward for the necessary computational eﬀort. The amount of reward decreases by a constant factor, which is halved each time the blockchain is stretched by 210000 blocks, this factor in the intention of the developers should roughly trace the rate at which the gold is extracted and fact places a limit on the maximum number of bitcoins in circulation, estimated at approximately 21 million

**If Bitcoin can be considered, from a theoretical point of view, a currency or a good is still the subject of discussion**, even if on 22 October 2015, the Court of Justice of the European Union has issued a law that decrees the exemption bitcoins compared to normal taxation of goods and services. In practical terms, the acceptance of Bitcoin as a medium of exchange has grown in recent years and at the moment it is accepted by thousands of commercial activities, even if we are very far from the exchange volumes of real currencies like the dollar. or the euro. As for the other aspects that usually concern the functions of a currency, the debate is more controversial .In fact, in order to accumulate an asset as a valuable fund, it is necessary that this asset be desired, or that the market believes in it and in its potentialities to such an extent that it is required. If we imagine putting our bitcoins in a box, it’s like saying that in this box there is value only if the people around us believe it. Bitcoin has gained popularity rapidly, but its value expressed for example in dollars is rather unstable**. Its volatility makes Bitcoin a high-risk investment, and ultimately because of the instability of its value, it is rather diﬃcult to use it as a unit of value for a good because prices should be updated rather frequently. We can conclude by saying that at this moment Bitcoin represents an excellent means of exchange, a very bad unit of value and a rather risky fund of value.**

**Does Bitcoin guarantee the user anonymity?**

**Bitcoin is based on pseudonymous identity, meaning that funds are not tied to real-world entities but rather bitcoin addresses.** Owners of bitcoin addresses are not explicitly identiﬁed, but all transactions on the blockchain are public. In addition**, transactions can be linked to individuals and companies through ”idioms of use”** (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses. **Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information**. To heighten ﬁnancial privacy, a new bitcoin address can be generated for each transaction. For example, hierarchical deterministic wallets generate pseudorandom ”rolling addresses” for every transaction from a single seed, while only requiring a single passphrase to be remembered to recover all corresponding private keys. **Researchers at Stanford University and Concordia University have also shown that bitcoin exchanges and other entities can prove assets, liabilities, and solvency without revealing their addresses using zero-knowledge proofs** (In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party can prove to another party that he/she knows a value x, without conveying any information apart from the fact that he/she knows the value x.)

Actually, one of the great promises of this technology is anonymity: the transactions are recorded and made public, but they are linked only with an electronic address. So whatever you buy with your bitcoins, the purchase cannot be traced speciﬁcally to you. This is handy for some, but the anonymity is by no means perfect. Security experts call it pseudonymous privacy. You can preserve your privacy as long as the pseudonym is not linked to you. But as soon as somebody makes the link to one of your anonymous books, the ruse is revealed. Your entire writing history under your pseudonym becomes public. Similarly, as soon as your personal details are linked to your Bitcoin address, your purchase history is revealed too. **A paper by Steven Goldfeder at Princeton University says the way information leaks during ordinary purchases makes it straightforward to link individuals with the Bitcoin transactions they make, even when purchasers use additional privacy protections. The main culprits are Web trackers and cookies**. Common Web trackers send information to Google, Facebook, and others to track page usage, purchase amounts, browsing habits, and so on. Some trackers even send personally identiﬁable information such as your name, address, and e-mail. In this way, information about a transaction leaks onto the Web, where governments, law enforcement agencies, and malicious users can readily collect and analyse it.

The question that Goldfeder investigated is how easy it is to use this information to connect people to their Bitcoin transactions. This process requires the eavesdropper to know an individual’s personally identiﬁable information-name and e-mail, for example and then to link that with a speciﬁc Bitcoin address. The team began by listing major merchants that allow Bitcoin transactions. They came up with 130 of them, including Microsoft, NewEgg, and Overstock. They then studied how Web trackers leak information from each of these sites during the purchase process. We ﬁnd that at least 53/130 of merchants leak payment information to a total of at least 40 third parties, most frequently from shopping cart pages, say Goldfeder. Most of this information leakage is intentional for the purposes of advertising and analytics. But the researchers also say some extra information is also sent. We ﬁnd that many merchant websites have far more serious (and likely unintentional) information leaks that directly reveal the exact transaction on the blockchain to dozens of trackers, they say. **Even when the exact transaction is kept hidden, it is still possible to make the link when the leak includes the amount and time of the purchase.** The eavesdropper needs to convert the purchase amount into Bitcoins using the exchange rate at the time and then search the blockchain for a transaction of that amount at that moment. This reveals the Bitcoin address of the user. Any other purchases made using that address are then trivial to track down.

There are a couple of additional factors that make this process trickier. The Web tracker might leak the cost of the product but not include shipping, so the total Bitcoin purchase may not be clear. There may also be a gap between the time the user viewed the page the information leaked from - the checkout cart, for example and the time when the purchase was actually made. Bitcoin purchases are time-stamped, so it becomes harder to track them down if the time is not known accurately**. The purchase amount is usually given in a local currency such as dollars or pounds and then converted into Bitcoin at the instant of purchase. Because of the large variability in Bitcoin exchange rates, it can be hard to work out the exact Bitcoin value if the purchase time is not known accurately.** All these factors make it harder to link individuals to their Bitcoin transactions, but it is by no means impossible. ”**We ﬁnd that unique linkage is possible in over 60% of cases for realistic values of these parameters**,” the researcher said.

There are ways to further hide Bitcoin transactions. **One of the most popular is CoinJoin, a service that links users who want to make similar payments and then allows them to pay together. This mixes their bitcoins, making it harder to identify them. But Goldfeder pointed out that if an individual uses CoinJoin to make several purchases in this way, it is straightforward to link them back**: ”If the victim employs 3 rounds of CoinJoin and the adversary observes two of the victim’s payments, he can link them back to her wallet (despite mixing) with 98% accuracy.” There are several ways buyers can protect themselves using tools such as Ghostery, AdBlock Plus, or uBlock Origin. These are useful but can sometimes miss trackers and at other times prevent purchases entirely. ”Such defences can be quite eﬀective, but they are far from perfect” said Goldfeder.

**Some comments about bitcoins and its blockchain technology**

**Bitcoin goes towards a global need for money** (can be spent anywhere), **combines the advantages of electronic money** (there is no need for physical currency) **with the advantages of cash** (no intermediary is used and therefore there are no problems of privacy / traceability of our expenses**) and with minimal transaction costs** (there is no intermediary to be remunerated). **Many researcher are convinced that in the future there will be a world cryptocurrency** because the world is going in the direction of globalization. Perhaps, indeed **almost certainly, it will not be the bitcoin**, also because bitcoin was built with an “old” technology (the new altcoin are more performing) and the quantum computing will make soon obsolete the proof-of-work based on elliptic curves. Another limit for the bitcoin is that is deﬂationary. For a currency is much better to be inﬂationary than deﬂationary: it must be more convenient for currency to be spent than to be stored waiting that increases its value. But the new altcoins overcome these difficulties.

A coin like bitcoin, in fact, if it were chosen as a world currency, would give several problems, among them:

 - just consider the problem of convergence towards the Euro in a fairly homogeneous economic area. It is a process started with the ECU in the 80s. It cannot be said to have been concluded. He caused ﬁnancial crises and forced the ECB to intervene with Draghi’s bazooka. **It is impossible, in this moment, to think to a world-wide currency, in such a non-homogeneous world context, without a central authority ready to mitigate the disruptive eﬀects.**

 - **the taxation of transactions**. Since the transaction is anonymous, it is not possible to know in which country it took place and a system should be invented in order to tax it and to attribute the taxes to the country in which they compete.

**Is the present value of the Bitcoin fair?**

**The current listing of bitcoins is the right one? Obviously not, we are in the presence of a ﬁnancial bubble** that can explode at any moment. But as always a ﬁnancial bubble is a way of getting rich for someone and losing a lot for many. Bitcoin, however, has its own reason to exist, so I do not think its value can completely cancel itself out. It has its own potential market, in some niches of world trade it represents a convenient payment method compared to the traditional ones, it has its charm in the most technological community and among the young people. The problems are:

 - **the regulatory context**

 - **it is necessary to ﬁnd who does the work of the miners**, so whoever takes on what the miners now supply, that is:

 a) hardware acquisition and maintenance,

 b) electricity supply

 c) connectivity

 d) the costs inherent in the physical structures where the hardware is to be maintained.

In early 2017, Harvard Business School professors Marco Iansiti and Karim R. Lakhani said **the blockchain is not a disruptive technology that undercuts the cost of an existing business model, but is a foundational technology that ”has the potential to create new foundations for our economic and social systems**”. They further predicted that, while foundational innovations can have enormous impact, ”**It will take decades for blockchain to seep into our economic and social infrastructure**.” In introducing the catastrophe theory René Thom tells the story of the young man who devotes his entire life to learning the sacred art of hunting the dragon, only to discover at the very end that the dragons do not exist. In the history of science and technology, this has often happened: the development of a beautiful theory (or a promising new technology) that does not ﬁnd applications. The impression (more than a impression) is that the blockchain technology will be able to face and win many and many dragons.