ʌNOLOGY: FIRST PART.

⸗, PRELIMINARY INFORMATION AND THE HISTORY OF THE BITCOIN

⸗TION OF BLOCKCHAIN TECHNOLOGY AND A BRIEF HISTORY OF THE BITCOIN

ė first part I will focus my attention on the blockchain technology and on its first product: the ocurrency known as bitcoin. In the second part I will speak about the applications (also the potential ⸗s) and about the bitcoin sons, i.e. the altcoins. More in detail in these first 10 hours, I will speak about ⸗e 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 2^8 possible keys. A 56-bit key would have 2^{56}, 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.