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:

$\sum 210000 \times (50)(1/2)^n = 21000 \times 50 \times 2 = 21000000$ 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;