Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών

-

Τμήμα Μηχανικών Πληροφορικής

(Εφαρμοσμένης Πληροφορικής & Πολυμέσων)

Πτυχιακή Εργασία

«Βιβλιογραφική Ανασκόπηση για το Ψηφιακό Νόμισμα Bitcoin»

Ονοματεπώνυμο: Βασμαριδάκη Ευθυμία Α.Μ: 3590

Επιβλέπων Καθηγητής: Παπαδάκης Νικόλαος

ΗΡΑΚΛΕΙΟ 2016

Copyright

Copyright © Vasmaridaki Efthimia, 2016. All rights reserved.

The graduation project entitled "literature review for the digital currency bitcoin», is the Thesis Conducted by the undergraduate student Vasmaridaki Efthimia, the period of the spring semester 2016. With every caution the copyright process of this work has been fulfilled. Also, the TEI of Crete and the supervising professor are not responsible in any case of copyright theft.

Thanks

This graduation project, "Literature Review on the Digital Currency Bitcoin» was written as a Thesis for the Engineering Department of Information Technology of the Technological Educational Institute of Crete. At this point I feel the need to express my sincere gratitude to those who contributed to the completion of this first effort. First of all, my supervising professor, Mr. Papadakis Nikolaos. I would also like to thank Mrs. Joanna Sygletou and Mrs. Despina Litsa and Mr. Dimitris Zoitas for their valuable assistance regarding the material and the translation of the thesis.

Περίληψη

Η αλματώδης εξέλιξη της τεχνολογίας και η αύξηση του όγκου των διαδικτυακών συναλλαγών, οδήγησαν την οικονομία στη δημιουργία ψηφιακών νομισμάτων με σκοπό να γίνει μια μέθοδος αγοροπωλησίας, πληρωμών και συνεπώς μορφή εναλλακτικού χρήματος γενικότερα. Διευκολύνει την πράξη αυτή, διότι, οι συναλλαγές γίνονται μέσω του διαδικτύου και όπως είναι κατανοητό ο κάθε ένας μπορεί να πραγματοποιήσει μια συναλλαγή με πολύ απλό τρόπο από το σπίτι του. Ωστόσο, δεν αποτελεί αποδεκτή μέθοδο πληρωμής σε αρκετές εταιρίες στον κόσμο. Μάλιστα, ακριβώς, επειδή πρόκειται για ένα ψηφιακό νόμισμα, που συναλλάσσεται μέσω του διαδικτύου δημιουργεί αμφιβολίες για την αξία του. Παρόλα αυτά, αξίζει να αναφερθεί ότι ίσως αποτελεί περισσότερο επένδυση παρά μια μέθοδο πληρωμών, με τη κλασική έννοια του χρήματος, όπως όλοι γνωρίζουν σήμερα, διότι η αξία του αυξομειώνεται ανάλογα με τη προμήθεια των χρηστών να αποκτήσουν τα κρυπτονομίσματα αυτά.

Summary

The rapid evolution of technology and the increasing volume of the online transactions, led the economy to create digital currencies in order to become a method of buying/selling and payments in general. This practice is facilitated because the transactions are being made via the internet and as it is clearly understood, everybody can carry out a transaction in a very simple way from home. However, it is not an acceptable payment method for several companies in the world. Furthermore, exactly because it is a digital currency that is being used for transactions via the Internet, it creates doubts about its value. Nevertheless, it is worth mentioning that it might constitutes more an investment than one payment method, with the classical concept of money as we all know today, because its value fluctuates depending on the willingness of the users to acquire this cryptocurrency.

Chapter 1

1.1 Money

With the commonly known terminology “money” we mean every asset that is used and is well known for any kind of payment. It is any object that is capable of being used by a society as a transaction / exchange medium, as a calculation unit in terms of purchasing power, in other words as a substitute of value. The value of money arises partly from its usefulness as a medium of exchange. The recognition of its market value is linked to its usefulness as a medium of exchange, therefore these two aspects of money are interrelated, the first is the cause of the outcome of the second and vice versa. Throughout history there have been various forms of money (they will be mentioned in more detail below) whose physical form is very different according to what currently exists in the mind of mankind. Societies created, create and will continue to create means / types of transactions, when there was / is no other, because the natural human needs instinctively arise.

However, to avoid any kind of misrepresentation it may be appropriate to determine with precision and clarity the distinction between monetary assets and non - monetary assets, which can be anything other than money. In contemporary economy the determination of this concept is very specific because anything else other than currencies, banknotes and deposits is not money. The total of coins and banknotes - worth mentioning that the banknote is synonymous with the term note - is known as the total of monetary circulation. However money is not only that, becausethe deposits of individuals in commercial banks, and the deposits of commercial banks in the central bank are also considered as money. For example, the check is considered to be one of the many forms of money according to the definition of money today. Furthermore, charging credit or debit cards is also considered as money. On the other hand, bonds and other similar debt instruments, securities, such as stocks and mutual funds is not acceptable to the economy as money despite the fact that it would be possible to deal directly.
For this very reason, various types of financial securities are called financial products.

1. 2 History of money

1. 2. 1 The emergence of money

In ancient times people were doing business with completely different means than the ones generally accepted in the modern economy. The widespread method at the time was actually the exchange of various goods. For example, the producer of a product exchanged their extra products to another producer's surplus products. This method of exchange of goods dates back to at least 100.000 years ago, although it should be noted that there is no historical evidence to show that the economy and the society were entirely based on this method. Several cultures around the world created and developed the use of some kind of currency in which the value of the material from which it was made determined its value. A unit of that currency also a unit of weight in those years, was called "siglos" or "shekel". This term came from Mesopotamia around 3000 BC. Furthermore, they started to use shells instead of money at states in America, Asia, Africa and Australia. Many objects were used instead of money during that era, from valuable metals were to shells and cigarettes to coins and banknotes. The first coins were made of bronze and then iron. The material from which the coin was made determined its monetary value. Then they replaced the iron with another valuable metal, silver. This was done by King Phedon of Argos, around 700 BC. King Phedon created this silver coins in Aegina and engraved a turtle on them, an illustration still used as a symbol of capitalism. These coins on which the turtle was engraved were widely accepted and were used as an international medium of transactions until the Athenian Drachmas took their place after the Peloponnesian War.

1.2.2. The Evolution of Money

The method according to which the value of the material, from which the coins were made, determined the general value of the coin, eventually evolved to the representative money that is well known to us all today. This occurred because the gold and silver merchants and banks issued receipts to depositors, writing the amount of the money that were deposited, and therefore, these receipts were established and were commonly accepted as a way of payment, and so they began to have the role of money. It is worth mentioning that banknotes were firstly used in China during the Chong Dynasty (it was an era of the Chinese history during 960-1279, succeeded a period of 5 dynasties and 10 kingdoms, and was followed by the Yuan Dynasty). These banknotes, also known as "Jiaozi" -a kind of chinese dumplings- evolved into debt instruments and their use began in the 7th century AC, however, during the same time, people continued to use "actual value coins". Right after that, the first banknotes were printed in Europe in 1661 and they were used alongside Stockholms Banco's coins. The advantages provided by the issuance of banknotes by banks were many. Transactions were eased in such a way and the banknotes were established as the most secure exchanging practice. In Europe between the 17th and 19th century, gold coins were replaced by this currency system mentioned above, where papers is the only medium of transaction. Papers (notes) that are actually able to convert to predefined, stable, gold quantities. However, their conversion into gold was discouraged, but nevertheless they legalized these "gold"

certificates as money. Later, in the early 20th century, almost every country adopted this monetary system, whereby each certificate they issued had a specific amount of gold for encashment. More recently, after the Second World War, these countries adopted the fiat money, whose value is determined by the value of the US dollar (USD). The fiat money, otherwise known as forced circulation money, is the payment instrument that is not covered by reserving other materials and therefore lacking of any asset value even indirectly. The US dollar in its turn is determined by the price of gold. The US government stopped converting dollars into gold and that was the cause, in a way, for other countries to follow the lead of the United States resulting to the majority of the world's money stop being supported with gold reserves.
Over the course of all these years since money or, even better, means of transactions, first appeared, we come to today at a point where technology has made a tremendous progress and gives us the ability to use digital, electronic, intangible currency. Currency that we are a able to conduct transactions with, the same way we are able to do with banknotes, coins, checks and all the means that are considered as money. There are several digital currencies that will be mentioned below. The most popular of them is the digital currency known as Bitcoin.

Chapter 2

2.1 Bitcoin history

Bitcoin is first mentioned in January 9 2009, in a document that was published with the signature of Satoshi Nakamoto. However, this currency's beginning was not rather nice because early technical problems occurred. There was a bug that allowed unlimited bitcoins to be created. Two years later, in 2011, the value of a bitcoin increased a lot, from $0,30 to $32. After that the value declined to $2. A year later, at the end of 2012, the cryptocurrency bitcoin succeeds to excite the interest of the media, and a variety of articles have been written for it since. A few services started to accept payment with bitcoins, some of them were OkCupid, Footler, Baidu and others. During November 2013, bitcoin in BTC[1] China surpassed the Japanese Mt Gox[2] and the European Bitstamp. It is the largest in volume stock exchange bureau for trading Bitcoins. The Bitcoin value increased significantly, reaching up to 900 USD in November 19th 2013. This was the result of a hearing held in the Committe of the Senate of the USA, during which an announcement took place saying that virtual and digital coins are a legitimate financial service. This hearing lead -in the same day- to the trading of a bitcoin at $1100 at BTC China. With about 12.000.000 bitcoins in circulation in November 2013, that price meant that the capitalisation of bitcoin is at least $7.200.000.000.

2.2 A Few words about Bitcoin

Bitcoins, (coded BTC or XBT) is a digital, peer to peer, currency whose function is not controlled by any central authority. It was named cryptocurrency for the following reasons, because it uses cryptography to control transactions and is decentralized so as to avoid double spending, something which is a common problem with digital currencies. Once every bitcoin is discovered from their production procedure, when the entire issue is completed, every individual and distinct transaction will be permanently enshrined in a public account, commonly known as a Blockchain. There is a specially adapted computer network from which the production procedure is done by processing blocks. The entities of these computers are known as miners and are rewarded, relevant to the transfer efficiency of the newly mined bitcoins, in their wallets for their mining expenses.

Bitcoins are basically saved in files, that are named wallets, and they are saved there via their connection. They can be saved in web services, in external storage device units, computers or mobile devices, or by printing them in paper.

It's good to mention that quite often the media have reported cases of bitcoin theft from the online wallets and from web services, claiming that the most secure and effective way to save bitcoins is in the paper printed wallets.

Specifically, in 2012, an analysis in The Economist accused the popular digital currency of being so popular because it is used for "cunning" online transactions. A year later, the FBI shuts down Silk Road service for their involvement in illegal drug trafficking. At this point it is worth mentioning that this gave rise to the FBI to control 1.5% of all Bitcoins currency in circulation.

Despite this fact, bitcoins are increasingly used for legitimate transactions, and this is actually in the merchants' interest because the transaction fees are lower by 2 to 3% compared to those imposed by credit cards. It is important to mention which companies are accepting payment by this method: OkCuppid, Reddit, Wordpress and also the Chinese giant of the online world, Baidu.

2.3 Satoshi Nakamoto

Satoshi Nakamoto is the creator (or possibly the creators) of the digital currency Bitcoin, as it has not been yet clear whether it is a real name or just a nickname. He, she or they, published a document in 2008 by the title "The Cryptography List", in HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/" HYPERLINK "http://metzdowd.com/"metzdowd.com, through which they describe the cryptocurrency Bitcoin. In 2009, version 1.0 of the bitcoin software was deployed, through which the network as well as the currency named Bitcoin was created. The creator(s) continued to contribute, as they say, in the release of Bitcoin software in collaboration with other developers. The community started to wear off in the mid-2010. Shortly after, Satoshi Nakamoto, handed over control of the source code and basic alert functions of the software to Gavin Andresen. Gavin Andresen, born in Gavin Bell, is the head scientist of the Bitcoin institute. He has access to the alarm key that allows him to transmit messages about critical network problems to all customers.

During the same period, Satoshi Nakamoto also handed in the control of the webpage HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/"

HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/" HYPERLINK "http://bitcoin.org/"bitcoin.org as well as many other sectors to prominent members of the bitcoin society.

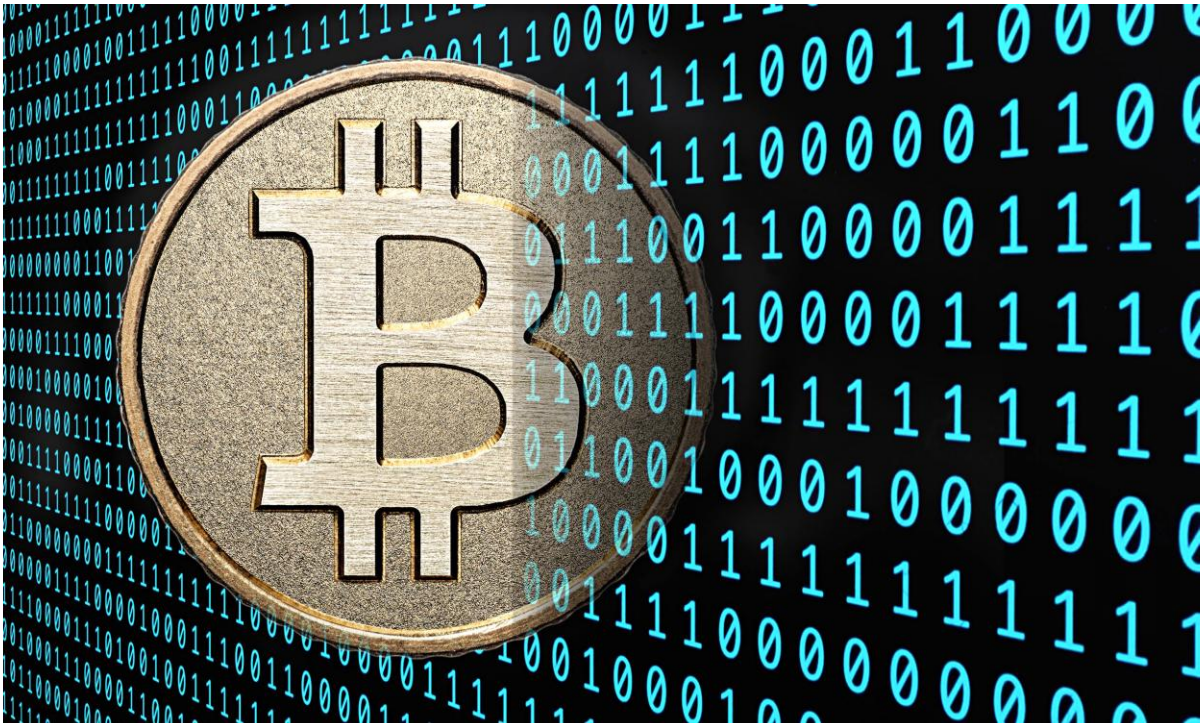
In addition, it is rumoured that Satoshi Nakamoto has 1.000.000 bitcoins, equivalent to 1.1 billion U.S. dollars.

Satoshi Nakamoto withdrew from the public in April 2011, leaving the responsibility of the code and the network growth to a thriving team of volunteers. The identity of the person or persons behind Bitcoin is still unknown. However neither Satoshi Nakamoto nor anyone else has control of the bitcoin system which operates under fully transparent mathematical principles. The invention itself is innovative and has already spawned new a science in the fields of distributed computing, economics and econometrics.

Chapter 3

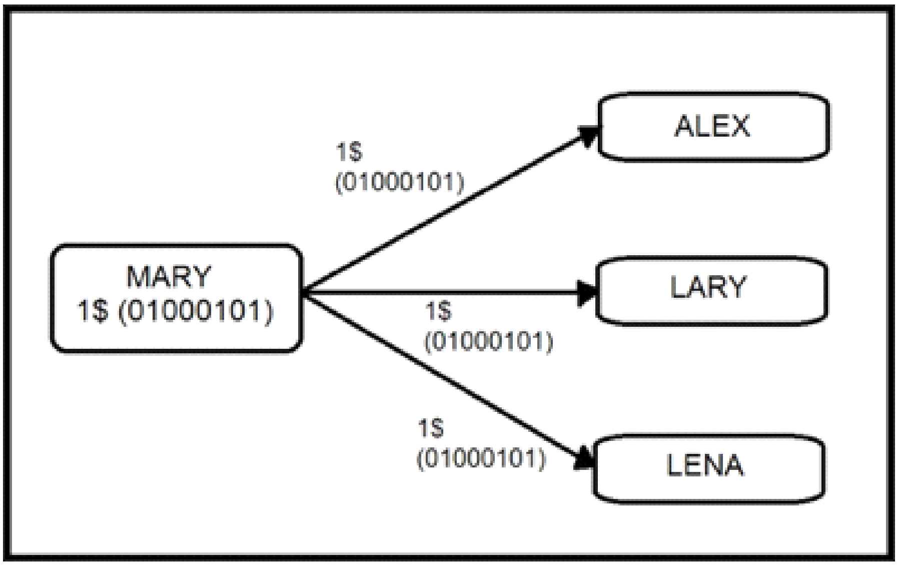
3.1 What is the digital currency Bitcoin

The digital currency Bitcoin is a collection of concepts and technologies, which is the basis for a digital money ecosystem. Currency's units that are named bitcoins are used for the value storage and transmission between the participants of the bitcoin network. Users of this currency communicate with each other using the Bitcoin protocol mainly through the internet, although it can be used through other networks as well. The bitcoin protocol stack, the available open source code software, can run on a wide range of computing devices, including laptops and smartphones, making this technology very accessible. Users of bitcoins can transfer them via internet just as the would with other conventional currency. For example they can buy and sell products, send money to people or organisations or even extend credit. The Bitcoins can be bought, sold and exchanged for other currencies in specialized exchange rates. In a way, we could say that bitcoins is the perfect internet money form. It is fast, safe and without boundaries. In contrary with traditional currency, bitcoins are totally iconic. There are no physical coins or even digital coins per se. Bitcoins are generated with the transaction that carry the value from the sender to the recipient. Bitcoin users have their own private key that proves ownership of the transactions via the Bitcoin network. Using this key, the value unlocks and passes to a new recipient. These keys are usually stored in a digital wallet in each user's computer. The only condition that is necessary for this transaction is the possession of the unique key that the user possesses to unlock the value and the bitcoins will be passed to his account. The whole process is entirely in the hands of each user. Bitcoins is a distributed peer to peer system, therefore there is no main server or a control point. Bitcoins are created through a process that is called mining which includes something like a competition where there are solutions to a math problem during the processing of the Bitcoin transactions. Each person that participates in the bitcoin network (everyone that uses a device that runs the full bitcoin protocol) can act as a miner using the full CPU power of his computer to verify and record the transactions. Every 10 minutes on average, someone is able to ratify their calculations, and they are rewarded with brand new bitcoins. Practically, mining bitcoins decentralises issuing new coins, performs a clearance in a central bank's functions and replaces the need for every central bank with this international competition. Bitcoin protocol includes merged algorithms that control the mining function throughout the network. The difficulty of the processing operation where miners have to perform is to record with success a block of transactions for the bitcoin network, which is adjusted dynamically, so that anyone would be able to manage on average every 10 minutes, regardless of how many miners are working on the same job at any time. The protocol also decides in half the rhythm at which new bitcoins are created, every four years and reduces the total bitcoin number that will be created in a fixed sum of 21 million coins. The result is that the number of bitcoins in circulation, is faithfully following an easily predictable curve that reaches 21 million by the year 2140. Furthermore it is not possible to print new money over and above the expected rate of issuing. Its worth noting that Bitcoin is also the protocol name and it is distributed as the biggest computing innovation. The first application of this invention is the cryptocurrency Bitcoin.

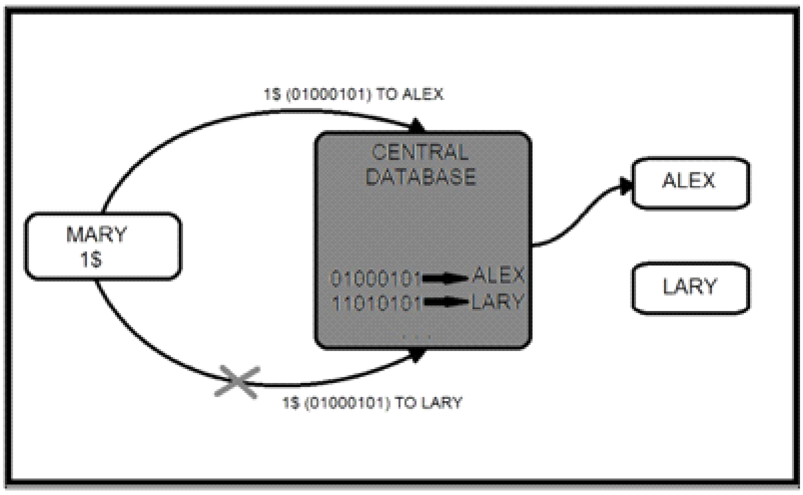


3.1 Software - Technology

Bitcoin is set up on an open source code. This code is public and accessible to make it possible to anyone to check the details of its operation. The fact that it is set up on an open source code gives the option to copy and develop a new software based on the existing, so it is possible to have various versions or distributions because anyone with the right skills can create a similar network by adding or changing the rules what he wishes. Establishing criteria for production and transaction of bitcoins, maintaining property information of the already produced bitcoins and the dynamical verification of the validity of the previous, are the goals that this software tries to achieve. The basic function of this software is running bitcoin transactions, transmitting information between nodes, and verifying their validity from the rest of the network. This software can be used for free and is available in all countries with the only condition of an existing internet connection. This network's power comes from its users' acceptance. The changes that refer to the code are proposed in the community but the network is created by the consent of the users and their acceptance. The transparency of the source code, the integrity, the transparency of the information being transacted, protecting the network from malicious attacks, producing limited bitcoins and finally the protection that the cryptographic algorithms provide are the main reasons that this software is accepted from current users and spread to new ones. The exchange value of bitcoins is shaped by the laws of supply and demand, without intermediate parts.The value that users find reflect the value they are willing to make in an exchange. The software and its developments consist the core of the bitcoin exchange system. The ability to exchange information with integrity regardless if it is accepted within the network, the limited availability and finite bitcoins quantity creates the basic requirements for a value exchange network. The right way to try and create a digital value in a particular data element is basically a series of 0 and 1. The problem with this approach is that digital information is easily copied without any basic cost. In the image below you can see the principles of double consumption (image 1.0)



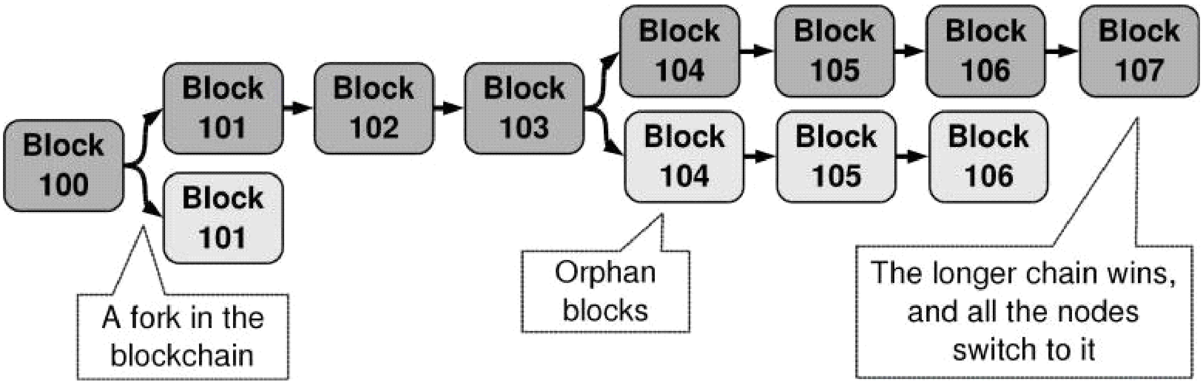
Suppose that Mary has a digital currency, represented by the binary number 01000101. She can transfer this value to Alex sending him a message with this number so that he has a copy of the number therefore the value of the currency. The problem is that nothing can stop Mary to send the same number to another user or to be exact to a many other users. So the digital value cannot be represented simply by a number because that makes it easy to be copied many times, therefore knowing the number has no value. As proposed by common sense, something that has value, has to be rare, therefore the challenge is to create something rare using digital technologies that allow perfect information copying. The next step for creating such a payment system is creating a central database containing the list of users and the capital each one owns.



Now if Mary wants to transfer a currency unit that is represented by the number 01000101 to Alex, she communicates with the server, runs through the main database and directs it to be transferred to Alex. If Mary tries to double consume this number, lets say to Larry, she will have to connect again with the server where it (the unit) will be checked. It will be found that this unit with this binary number does not belong to Mary anymore therefore she has no right to spend it. The main database solves the problem of double consumption. There are other matters connected to the main database though. First, all users should be registered in the central server in order for this to work. Then, the central database recognises the identity of every user and collects their financial history. Also a central database can easily become a target for malicious attacks either from inside or outside factors. If the person(s) attacking can gain control of the central data then he cone change property of capitals and steal them from their rightful owners, or even create new funs (points) and define them to him/her/theirselves. Perhaps the greatest disadvantage of a main server is that it consists of a single point of failure (as seen in image 3). the payment system can easily be dismissed by shutting down the main server.
Some early digital payment systems were based on the concept of a central database that would maintain every user position, like e-gold, that is a digital gold coin that operates from Gold & Silver Reserve Inc.

3.2 The blockchain

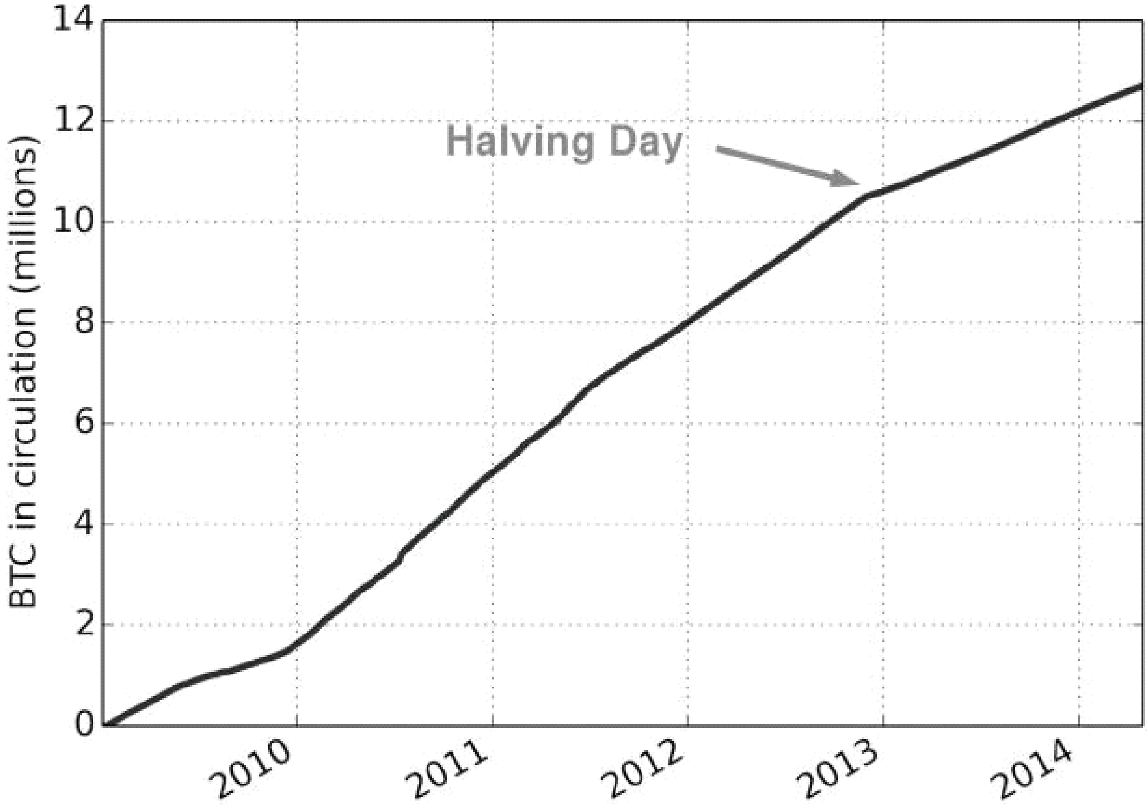
The distributed data base for Bitcoins is called a Blockchain. Transactions are grouped approximately every ten minutes. These groups of transactions are listed after group of chains hence the name Blockchain. It can be a peculiar way to record information in comparison with a conventional relational database. The blockchain is designed to be flexible in case of an attack on the network. The groups are linked as to create a history file of the transactions that cannot be changed. The link between the groups is encrypted and cannot be attacked unless the person attacking has unlimited computing resources. The blockchain is undoubtably the most significant innovation introduced by Bitcoin. It is the link that makes peer-to-peer digital coin distribution possible. The blockchain is basically a distributed database that holds all of Bitcoin transactions since the beginning (January 3rd 20019) and is a method that ensures this database. It maintains a secure list of every transaction ever made. However there is a question as to where a particular transaction is available to spend which is not directly found within a blockchain. The software that uses the blockchain, such as mining nodes, or wallets, is something that must be analysed by the Blockchain so as to extract the relevant information. This information, exported from the Blockchain is usually fed into a database. For example, the node of the Bitcoin software uses LevelDB, a “tore” key-value which will keep a copy of the transaction that has not occurred. The blockchain uses proof of labor to ensure the distributed data base. This means that the blockchain is secured towards any possible violation from the computing power that has been implemented for its creation. A user that wants to attack and change the blockchain, has to use equivalent computing power to all the power that has been used from the beginning of the transaction. Furthermore, the intruder has to overcome the legitimate bitcoin network, which keeps adding entries in the distributed database. It is easy to set up the block difficulty and this depends on the increase in the number of zeros of the binary digits. The bitcoin protocol adapts its difficulty every 10 minutes. This kind of difficulty is part of the regulations of bitcoin and is encrypted for every client of the bitcoin network. The block difficulty is adjusting every 2016 blocks or approximately every two weeks. The adaptation takes into account the change in the total CPU power of the network since the last adjustment. When the power of mining is added to the network, the blocks will adjust the difficulty in less than 10 minutes. However the difficulty will adjust to a higher level, but the network power will decrease. The innovation introduced by bitcoin is the combination of time-stamping and hash cashing as proof of labor (Conrad Barski, Chris Wilmer, 2014). The blockchain is a constantly growing chain of blocks. Every blocks includes a group of new transactions and a link the previous block of the chain. The new transactions in the network ar gather into the block that attaches to the blockchain. It is noted that the old transaction is still in the blockchain: the old blocks are never removed from the blockchain so the blockchain can only grow in length. Every block includes a special transaction called monetary base, which is the first transaction in the block. It also has only one transaction of inflow that is not linked with any other inflow transaction and it serves no purpose. On the other hand, the monetary base has many outflows. The sum of the output values is equal to the block reward as well as the sum of all charges recorded from the transactions gathered in the block. The blocks usually include many transactions outside of the monetary base. But a valid block can be created without including any other transaction made outside the monetary base. Actually, this type of block was the most common at the beginning of the bitcoin network, when very few transactions were made. These empty blocks help to ensure the blockchain and assign the miners their reward. The miners can select which transaction will include in the block mining and usually select based on the charging. The process of the block resolution is called mining and is relevant to the extraction of precious metals. The miners are rewarded with the new currency. This analogy although useful can be time consuming. The block reward is set by the protocol and is not affected by the number of minders or the labor they produce. In contrary with the extraction of precious metals, investing in increasing the miners will not increase the bitcoins in circulation. Investing in increasing the miners will increase the total fragmentation rate, decreasing this way the rates of the former miners, keeping the whole reward for the continuity of the network. A block that precedes another one is called parent block. Every block indicates its parent to the blockchain adding fragmentation in the data structure so the blockchain keeps the blocks in chronological order. The first block in the blockchain is called genesis block and was created by Satoshi in January 3rd 2009. The ordering of a block in the blockchain, starting from the genesis block, is called block height. The last block that is added in the blockchain is called blockchain head. New blocks are added over the blockchain head. A "fork" is created when two miners reach on a new block at approximately the same time. Both blocks solve the partial fragmentation inversion problem but only one of them can be part of the longterm chain. The block that is rejected is called orphan block.



This happens when there is a network separation and miners believe that one branch of the fork is the legal blockchain while the rest follow the other branch. The protocol define that the correct blockchain is the longest, so miners are motivated to stop working once it's obvious that the block is going to be an orphan because it would be a waste of time to continue working in that kind of branch. There are forks which find their solution quickly and usually only in one block. The average of forks is around 2%, for example for every 50 blocks there is one fork in the blockchain. Forks in more than one blocks are quite common. The transactions included in a block of a fork are not lost. When a fork is lost and the blockchain branch is rejected, the transactions in it (the branch) are inserted again in the unconfirmed transaction memory pool, ready to be included in the next mining block. Some of these transactions can already appear in a legal branch's block of the fork. In this case the transaction is rejected and is excluded from the unconfirmed transactions of the memory pool. Every analysis of the fork produces winners (the miners that solve the block in the accepted branch) and losers (the miners that solve the block in the non accepted branch). The protocol avoids to have a central party or group that will decide for the accepted branch, according to the decentralisation philosophy of Bitcoin. The bitcoin protocol solves the fork in favour of the largest blockchain. The length of the blockchain is measured by combining the difficulty of every blocks in the chain. If the difficulty of the blockchain was measured by the number of blocks, one that would want to attack the system could create many available blocks with small difficulty than the legal blockchain, so they would win the blockchain 'race' by cheating. The bitcoin network is consisted of nodes. These nodes are computers that are connected to the internet, running the bitcoin software. The bitcoin network is a peer-to-peer network: every node is uniformed. The nodes receive transactions and blocks from other nodes and transmit these transactions and blocks to other nodes. Every node keeps a complete copy of the blockchain. A new transaction that has not yet been included in a block is called an unconfirmed transaction. When the transaction is included in a block it is called a confirmed transaction. If the transaction is confirmed, it depends on the degree: the more blocks are added on the blockchain top the more difficult it is for a double consumption attack to occur against a a transaction. Finally, other than the complete copy of the blockchain, the node also keeps additional databases like the memory of non-spent outflow transaction or the non confirmed transactions from the memory pool, so that the node can swiftly validate new transactions and blocks that have passed the mining process. If the transaction or block is valid, the nodes inform the database and transmit to the connected nodes. It is important to notice that a node doesn’t have to trust other nodes because it validates independently every information that it receives from them.

3.3 Mining

Mining is the process of adding files in the blockchain. Miners contribute with the authority they have on their computers to solve the files that are added to the blockchain. The network rewards the miners with the fees that are collected from the transactions that are included in the file. The miners solve the defragmentation problem with partial inversion. For a solution to be found, the mining software usually increases the nonce of the fils and runs the algorithm, which proves if the selected nonce creates a right defragmentation, in other words a defragmentation that meets the requirements. The typical optimisation that is used from the miners is for the defragmentation of the first segment of the head of the file, that includes the previous defragmentation of the file and the Merkle tree, to be pre calculated. This part of the head of file is constant through the mining process and therefore it can be saved in a buffer stock. One of the advantages of the mining mechanism is the early reward of the ones that adopt it to support the network. Mining is similar to a marketplace with perfect competition as long as there is profit. New incomers will join the market until the profit chance is eliminated. The difficulty in mining is constantly increasing while more and more miners are joining the network but the sum of the reward from the files remains the same. During creation of Bitcoin, the reward was 50 bitcoins. This reward divides in half every 210.000 blocks or approximately every 4 years, to comply with the rate of creation of money specified in the protocol. Please note that issuing new bitcoins is not a smooth process, as the introduction of new producing capacity of mining temporarily increases the rate of creation of new positions per class until the feedback of the catching mechanism. Therefore, according to the increasing rate of the network defragmentation, issuing new bitcoins is somewhat increasing. At November 28 2012, a month before the timeline, the reward was decreased in have to 25 bitcoins.



Bitcoin is a peer-to-peer network where anyone can connect to and start mining right away. New incomers don't have to ask permission or to get attached to a set of rules or regulations before they join the market. Neither can the incumbents conspire to hire new participants, thus, new investments will be listed in the competition to get the file reward, reducing the pay of all miners, which are already in the network. So for the scenario of increasing the bitcoin value, or the increasing technological progress, miners will have to keep increasing the fragmentation rate in order to achieve the save reward, in a process similar to the Red Queen Effect. This process will continue until the limit cost of the last miner will be equal to their expected profit. At this point the network has reached a balance, which can be disturbed only by some outer factor, like a further increase of the bitcoin value.

Technological advantage. This technological advantage could come from either a new innovation in the application of the algorithm “proof of labor” SHA^2, either could come from a miner following an optimised production process, the same way a chip producer comes in the business world of mining.

Hedging Bitcoin Volatility. A miner has an advantage if in place to compensate the variability of a bitcoin value more efficiently than their competitors. Every miner can compensate the instability of the bitcoin value using bitcoin futures. At this time this market is almost inexistent. This advantage could be specifically significant during the period that the bitcoin value is in remission and the competitors are forced to close to this price. Even more, when a miner is in place to cover the variability of their expenses could demand an even lower rate of return of his investments.

Lower electricity prices. Miners that are in place to ensure lower prices of electrical power have a cost advantage. Bitcoin mining is very likely to migrate to places with plentiful and with a low cost electrical power, like for example Iceland. This possibly could decrease the environmental impact of bitcoin mining because, as a place with a lower cost for electrical power, it can produce environmental friendly resources like hydroelectric installations.

Briefly, entry barriers in the mining business are generally low, because there is no way for the incumbents to find the means to prevent the web entering the new competition. Therefore, the percentage of internet fragmentation will probably be stabilise in a percentage where mining rewarding will cover only the limit cost of the mining equipment. This limit operating cost includes electrical power cost, data centre renting, cooling cost, maintenance cost, and others. However there is the cost of depreciation of equipment or opportunity cost. It is worth mentioning that ASIC it is the only sustainable technology today that optimises the bitcoin mining and in fact there is no other alternative.These factors, combined with the delay in manufacturing mining equipment could create a “bang” in the mining business.

3.4 Wallets

The software that is in place to help a user to manage his funds is called a wallet. The functions of this software is to keep securely the user’s private keys, the creation of the transactions that are transmitted to the network and then gather the input and output transactions so that the funds balance can be available for the user. Because a user can be can be the owner of many addresses most wallets are ready to manage multiple addresses and therefore can sum all funds together. The software can create new addresses when it runs for the first time. Creating a bitcoin address is easy and immediate. The wallet can also materialise the encryption protocol as to sign a transaction with the private key. Private keys are usually kept in the device. Losing these keys forbid accessing the user’s funds. The funds are not yet distributed but without the private keys there is no way to sign and register a transaction and therefore they are considered lost. So, it is recommended to keep backup files of the created private keys. Most wallets help the user to create a digital safety backup. Another wallet danger are intruders that are persons not authorised and their purpose is to get in their hands the private keys. If an intruder attacks in order to gain access to private keys, he could send funds to addresses that are under his control. Therefore it is ever so clear how important it is to secure private keys that are saved in devices connected to the internet. Many wallets offer encryption of the private key before stored locally. This reduces the convenience to the user who has to type to access password to decrypt the private keys before using them, just like it happen while sending a transaction. In case that the device is in danger, the intruder will be able to get only one copy of the encrypted private keys.

3.4.1 Offline Wallets

Usually a device that has a wallet, is connected to the internet, in order to communicate with the bitcoin network (which takes into account the state of the account, the transaction transmittance, the confirmation observation and so on). What mentioned before is called an online wallet or “hot” wallet. Every device that is connected to the network is reasonable to be in some kind of danger, and is good to keep wallets that only have funds for every day use. The rest of the user’s funds should be kept in offline wallets for better safety, whose private keys won’t be accessible from the internet. Private keys that are kept in a temporary pause should be inserted in a wallet (offline or online) before accessing the fund.

Paper wallet: Another way for users to create a temporary pause, regarding private keys, is for them to be printed in a piece of paper where they will be safer in case of theft. These are called paper wallets, although technically they are not wallets. in a paper wallet, private keys or bitcoin addresses are usually printed with the private keys, so the paper wallet can be defined easily, without needing a private key to be entered. If private keys are created randomly, like they are in the core of a bitcoin wallet, then a copy of every private key should be printed.

Hardware wallet: are the devices that store private keys through which transactions are made. These private keys never leave the device and so it is not possible to be confiscated by a malware software in the user’s PC. Hardware wallets communicates with a software wallet the client has in a PC. This client can be either a program that is a wallet or a digital wallet that runs in a web browser. In any case, the client acts only as an intermediary between the hardware wallet and the blockchain. Some projects of the software wallet include support to hardware wallets. Transactions are sent from the user’s wallet to the PC and then to the hardware wallet through some kind of connection, usually a USB. The transactions that are carried return from the hardware wallet through the same connection. Hardware wallets have usually a small screen that show information relevant to the transaction, and some buttons that give users a the choice to decide if they will sign a transaction or reject it. In case a malware software is installed in the user’s PC it is possible that it will change the transaction information that are sent through the hardware wallet. The wallet’s screen shows details for the transaction which means that there is a protection against this type of attack. Its s also common for a password to be required so that the transactions from these connections to be accepted.

3.4.2 Web Wallets

Web wallets are online accounts connected to the internet with an external provider, which allows the user to be able to deposit their money. These funds are controlled from the wallet web provider. Through identity verification with the wallet web provider, the user has later the ability to access these funds, meaning he can make transactions. The main advantage of a web wallet is no other than the fast and easy registration. Creating private keys is done by the provider of this wallet, reducing this way the obstacle for new users to enter. There are many other advantages like lower cost for transactions or the ability to make transactions through the save platform in real-time and with no fees. Web wallets are like bank transactions that are made through the internet, meaning that the funds are kept from the provider of the web wallet. However, in contrary to the bank’s policy where deposits are covered with bank deposit insurance, the user cannot use legal ways against the provider of the web wallet who can possibly disappear with the fund. Furthermore, providers of web wallets are not thoroughly examined, like banks are, and this is possible to increase doubts regarding their credibility. Safety practices for the web wallet providers or their exchanges are similar to the practices that refer individual users, where they should keep only the funds they want to spend daily and keep the rest of their fund in an offline wallet or in a temporary pause. Using web wallets affects the user's private life a lot. Although the user anonymity is maintained because the addresses used for the transactions have no direct relation with the user, the word (anonymity) cannot have the 100% of its meaning because the web wallet provider usually keeps a record of the transaction and this way the user personal information is kept.

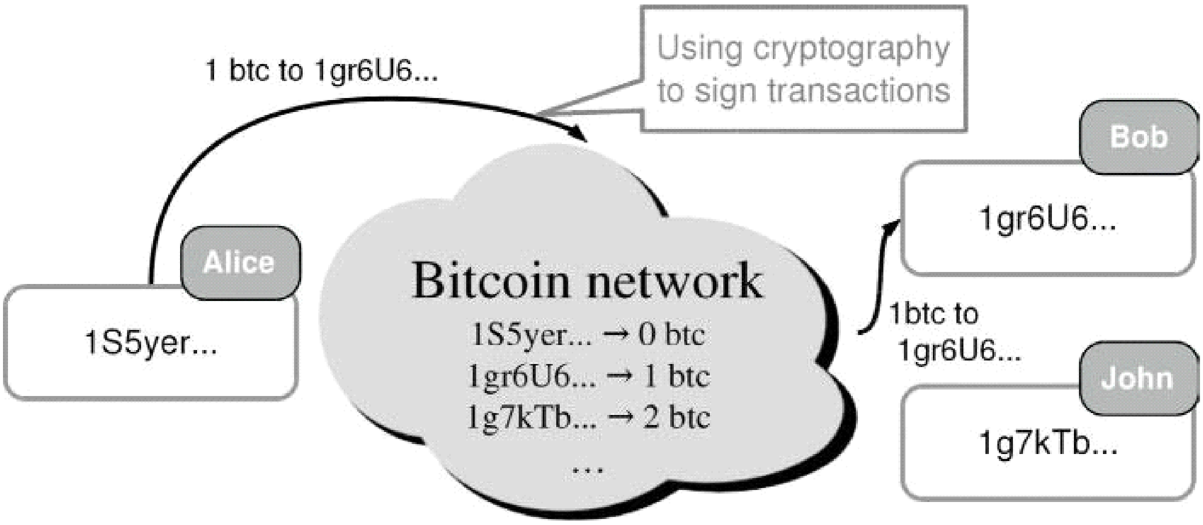
Hybrid web wallets are the web wallets where the private keys are kept in the user's PC but the management of the software is made but the service of the wallet provider. The transactions are initiated by the users, are announced firstly to the wallet provider which then publishes them to the blockchain. The advantage is the user's small exposure to the service provider and the disadvantage is the increase of cost for maintaining a safe user system.

3.4.3 Brain Wallets

Brain wallets have the ability to create a private key from the defragmentation of a large access code or a access phrase. Private bitcoin keys can be 256bit in size so that a defragmentation function that produces a 256bit piece, like SHA256, can be used. The access code of such a wallet doesn't have to be stored in a device because it is stored in the users memory, hence the name of the wallet. This has the advantage of no safety backup copies, provided that the user is in place to remember the access code. The access code should also be inserted in a real wallet so that the user can access the funds. Brain wallets have a large disadvantage that is reasonable to discourage users. They are subject to wild attacks through which is possible to steal all the money from the wallet in case of success. Such an attack tries many access codes and it checks if the address produced from the code exists and if there is any money in it. Chances of success from these attacks are very high.

3.5 Transactions

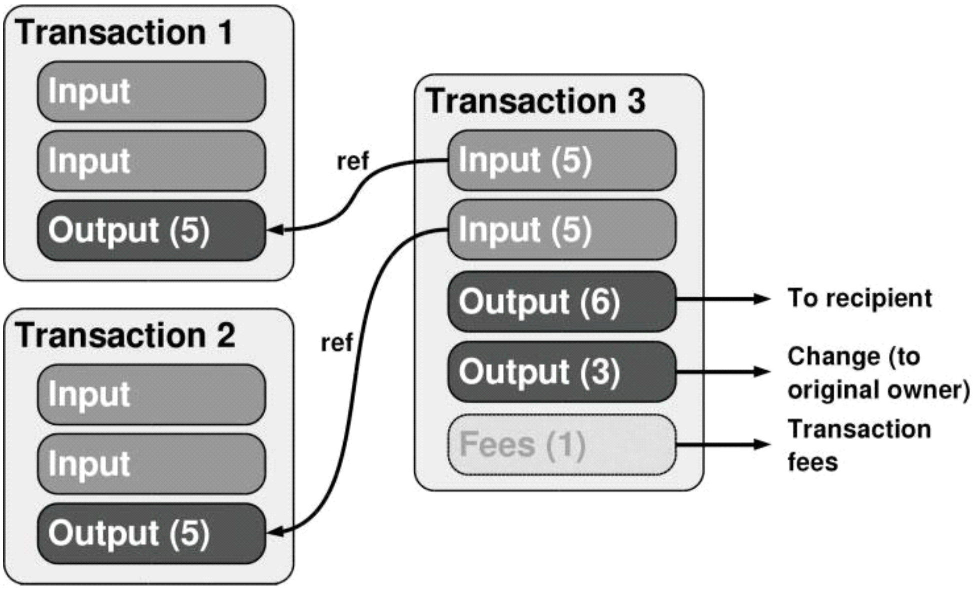
At the bitcoin network centre there is a decentralised universal that included each user's balance. Bitcoin identifies the users with long strings of letters and numbers like “13mckXc…”. An address is the public place of a public-private cryptographic key. The private part of the key is under the user's control.



The above schematic shows how a user (Mary) sends some funds to another user. Mary uses her own private key to sign a message saying “I want to send 1 Bitcoin to 1gr6U6… that belongs to Alex”, which she sent to the network. Let it be noted that Mary doesn’t specify the user she wants to send the funds but the address that will receive the funds. So Mary has to discover Alex’s address with other ways. When they get Mary’s message, the network nodes follow the following steps:

- They verify that the signature is correct. If not they reject the message
- They check that the address that runs the transaction has enough funds to be charged for the transaction. If there are not enough credited funds to the address the transaction is cancelled.
- Finally they update the database, retracting the funds from the one address and crediting them to the other.

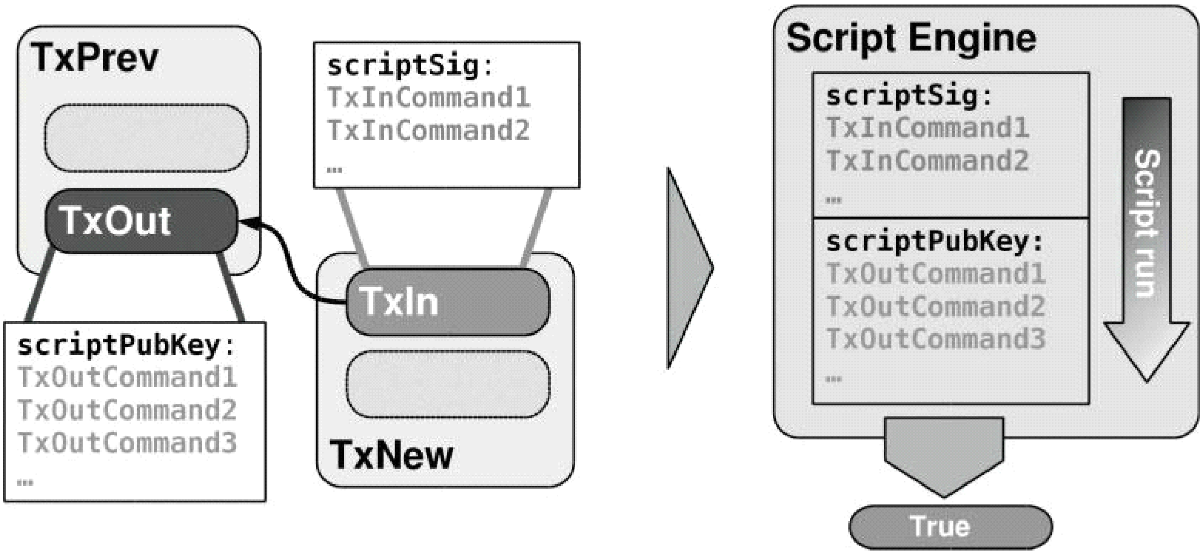
A basic detail is that the network nodes do not know the identities of Mary and Alex, they are identified only by their addresses. Bitcoin users are identified by the username: Bitcoin provides pseudonymity. Another basic detail is that the addresses are not given by the network. They are created in the users’ devices when they run the bitcoin software that encrypts public and private keys. While public and private keys are interdependent, they have to be created jointly and locally in the user’s device. The address generation process is simple and can be made almost instantaneously from any device such as a laptop or a smartphone. There is no restriction in the number of addresses a user can create. Actually it is recommended that the users create many addresses to strengthen their data protection. It is not mandatory for someone to signup to use Bitcoin. Actually, new users don't have to announce their addresses to the network as to receive funds. A user, let’s say Alex, can create an address and announce this address to Mary with other means, like an e-mail or a by coupling two smartphones. Mary can now send funs to Alex and the network will accept the transaction even if the address is new to it. In the central system, funds are kept from a central entity that also keeps the means to check these funds, reporting with the change of the registry to the universal. In contrary, in a non central system, the private key that gives access to the funds is exclusively in the hands of the end user. Bitcoins do not live in the user's PC. They are entries in a distributed data base called blockchain. Transactions are consisted of a list of inflow transactions (TxIn) and a list of outflow transactions (TxOut). Each outflow has two data parts: a value and its beneficiary address. This address comes from the public key. Only by this way the owner of the private key can unlock the funds that are stored in the TxOut. To release the funds, the owner of the private key has to sign a transaction sending the funds to a new bitcoin address. The outflow transactions keep record of the previous outflow transactions and a signature that proves that the previously referred transaction funds can be spent. This signature has to be made with the private key supported by the public key of the bitcoin address. If the signature does not match the transaction is considered invalid and is rejected by the network. For a transaction to be valid, the sum of the inflow amount has to be equal or greater with the sum of the outflow amount. The difference between inflows and outflows, if there is one, is the charge for the transaction. Transaction charges are gathered by the miners that include the transaction in a block. Outflows in a blockchain can be spent only once and their full amount should be paid. If the amount of the outflows is greater than the amount spent the transaction does not give change. The sender of the transaction can gather change adding an address of change as an additional outflow in the transaction. The event that an address of change is usually controlled by the sender of the transaction can actively be used from the mining algorithm data that is applied in the blockchain. The address from where the funds come from can be used as an address of change in a transaction but it is recommended for a whole new address to be created for every transaction in order to strengthen data protection.



In the diagram above we can see an example of transaction. In this example the sender wants to send six Bitcoins to the receiver. The sender though doesn't have in his disposal an outflow transaction with the exact number of six Bitcoins. He only controls two outflow transactions with five bitcoins each. So he creates one more transaction that groups the previous two outflow transaction and sends to the receiver six bitcoins. The sender adss an outflow transaction under his control to receive the change (3 bitcoins) and leaves one bitcoin as a transaction fee for the miners. Before he sends his transaction to the network the sender has to register these two outflow transactions to prove that he controls the address suggested by them. The transaction is afterwards sent to the network. The first network node that receives the transaction validates it. If the transaction is valid the node sets it free for the next network nodes. To validate the credibility of the transaction the node follows this steps:

- It checks that the previous outflow referred by the transaction does actually exist and that is not spent. The node continues checking consulting the unspent outflow transactions.
- It also checks that the sum of the inflow amount is greater or equal to the sum of the outflow amount. It makes sure that the transaction doesn't spend more than the available inflows. The difference of the sum of the outflow amount and the sum of the inflow amount is considered to be the commission left for the miner and is included in the monetary base of the transaction.
- Finally it cheese that the signature fore every inflow is valid, that every inflow is registered with a private key conjoined with a public key and both comply with the suggested address.

Up to this point outflow transactions are considered to be sent to a bitcoin address. Every outflow transaction creates a mathematical puzzle that has to be solved in order to “pass” the exit. For the puzzle to unlock the funds and and the puzzle’s solution are represented by two scenarios. The scenario tat creates the puzzle is called “scriptPubKey” because it is the sector of the scenario that includes the public key. The puzzle that solves the “scriptPubKey” therefore unlocking the funds is called “scriptSig” because its the sector of the scenario that includes the signature



In the image above we see the process in which an outflow is spent. An outflow (TxOut) creates a “scriptPubKey” that has to be solved in order to spend the funds included in the outflow. The protocol checks that the “scriptSig” solves the mathematical problem created by the “scriptPubKey”. For it to to this, the protocol creates a full scenario by joining the “scriptSig” and the “scriptPubKey” and runs it as a whole. If the final result is true then the input is considered valid. If the scenario fails in the middle or if the final result is false the, then the transaction input is invalid an all the transaction is canceled and rejected. Closing this chapter, the main ways of transactions are the following six:

TX_PUBKEY or pay-to-public-key. The “scriptPubKey” of this kind of transaction is [OP_PUBKEY OP_CHECKSIG]

TX_PUBKEYHASH or pay-to-address. The “scriptPubKey” of this of transaction is [OP_DUP OP_HASH160 OP_PUBKEYHAS OP_EQUALVERIFY OP_CHECKSIG]

TX_SCRIPTHASH or pay-to-script-hash (P2SH). The “scriptPubKey” of this kind is [OP_HAS160<20-byte-hash> OP_EQUAL]. A non standard transaction is entered in the “scriptSig” of a P2SH is not allowed.

TX_MULTISIG or multi signature transaction. The “scriptPubKey” of this kind of transaction is [m sig1 … sign n OP_CHECKMULTISIG]. This transaction is considered standard if n≤ 3 and m≤n

TX_NOTSTANDARD if none of the above transactions.

The first five transactions are considered standard transactions. Up to now only classic transactions are promoted by the nodes to the suggested software of bitcoin. To include a non-standard in a blockchain you have to make a deal with the miners and it is included when the miners solve the block.

4.1 Alternative currencies

Alternative currencies are the ones that have copied many of bitcoin’s characteristics. Most of these coins are based on the source code of bitcoin with some edits. It is accepted for the code of bitcoin that is released under an open source code license to be copied and altered to release a new cryptocurrency. Many developers have done this exact thing, creating many alternative currencies. Bitcoin development was conservative and keeps a value, emphasising in avoiding potential faults. In contrary with Bitcoin, alternative currencies usually don't have restrictions in th production system, like for example demanding compatibility that allows them to try new micro settings and characteristics. The following currencies will be mentioned and analysed:

Litecoin (LTC): It is undoubtedly the most successful alternative coin issued in 2011 and by the time this was written the currency had a capitalisation in the order of 5%. Some time it is referred as the “Silver to Bitcoin’s Gold”

Peercoin (PPC): This currency was introduced in 2012. Its basic innovation is that it uses a hybrid proof of participation in functioning the system. It has a system that proves the participation of new files analogous to the mining and the owners of the coins in proportion to the number of the coins checked. Proof of participation doesn’t come from solving a defragmentation problem with partial inversion and this way minimum electrical power consumption is needed. For this reason Peercoin is considered to be a “green” Bitcoin alternative.

Freicoin (FRC) issued in 2012. It is an alternative coin based on Bitcoin with the basic difference that it has an overdue tax. Demurrage is applied as a tax on the transactions that withholds a certain cluster out of freicoins. This cluster increased according to the time passed from the last transaction made with freicoin. This way, demurrage acts like a negative tax on the owners of coins. Freicoin applies a yearly overdue tax in the order of 5% and depends on some movements in the web. Freicoin is a tribute to the monetary system Freigeld suggested by Silvio Gesell.

Namecoin (NMC): It is as much a cryptocurrency as a decentralised store of key/price that is used as an alternative DNS address that have to be solved with an IP Address.

Primecoin (XMP): issued in 2013. Prime coin’s main innovation is proof of function that produces scientific results. This contradicts with most alternative coins, regarding the proof of work, like for example SHA256, whose results have no actual value other than assuring the blockchain.

Auroracoin (AUR): issued in February 2014. It is clearly a branch, meaning that is based on the characteristics of Litecoin. It’s basic innovation is not technical but concept-wise. Aurora coin’s 50% is pre-mined and given to the Icelandic people, and the other 50% of the monetary value is given to the miners.

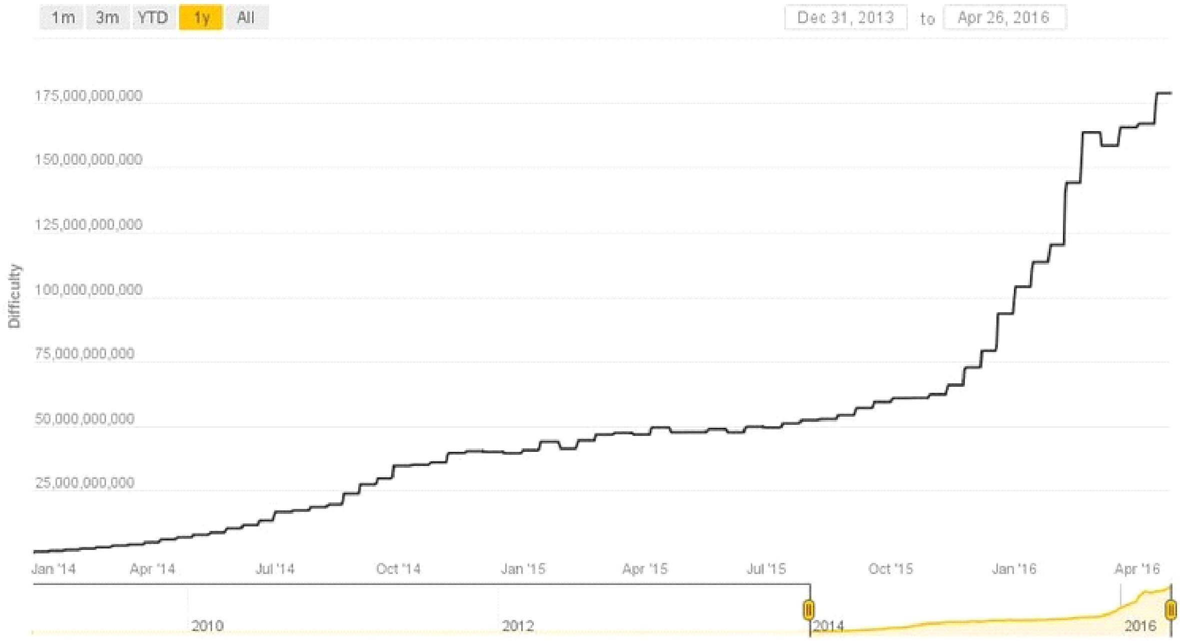
4.2 Bitcoin compared to other coins

Bitcoin is a virtual coin. The bitcoin gateway seems to be like other payment gateways, like credit cards, but above all these it is absolutely different. It has not got any owner, its purpose is not gaining money, so no one can take advantage of the payments that take place through it. Its structure is a peer-to-peer structure and for its successful completion many computers are needed.

5.1 Bitcoin’s disadvantages

5.1.1 The speculation

The speculators expect the bitcoins popularity to be broaden through the raise of its value in order to be an object of negotiation in investments. Nevertheless, the fact that this coin’s value depends on the users’ acceptance and there are security gaps so a hacker can easily access users’ data, creates doubt. It’s worth mention that there are only a few bitcoin derivatives so some additional future contracts of multiple currencies are offered. Furthermore, some investment funds have shown their interest in bitcoins, for example Winklevoss made a personal investment for 1.5 million dollars and Peter Thiel’s Founders Fund for 3 million dollars.



5.1.2 Bubbles

There is a statement that bitcoin gains popularity in countries that face currency problems, as it can be used for inflation circumvention, capital controls and international sanctions. For these reasons some people in Argentina and Iran widely use bitcoins. Professor John Quiggin of the University of Queensland has mentioned that bitcoin, from its first design, has no inherent value so it is maybe the best example of a “bubble” which is globally known and forewarns of a future annihilation of bitcoins value. Also, some economics experts mentioned that in Cyprus in the economic crisis in 2012-2013 there was a raise of bitcoin usage. A good-to-mention example is that of a Norwegian who bought 5000 bitcoins for 20 euros, and in 2009 their actual value raised to 650.000 euros. The Portfolio Manager of an Investment Company named Glendevon King Asset Management in London, believes that it is impossible for this coin to get a raisional value. As it is an easily transformed virtual coin,it has many characteristics of a “bubble” coin and that’s the reason why its value raises from 2 to 30 dollars and vice versa really easily. Many analysts uphold that its ejection of value in 2011 was due to Russian and Cyprian investors who were buying bitcoins with the perspective of an economic crisis in Cyprus. Bottom line, with the “haircut” of the bank deposits, bitcoin seemed to be a good alternative of euro.

Bitcoin was created in order to make it easier for users to complete online transactions through the Internet. The raise of its value in the last years is due to the lack of reliance on the bank systems, owing to the Cyprus economic crisis, and also due to its “safety” as it does not depend on any bank institutions or government agencies and the anonymity that it offers. For these reasons, Bitcoin use is considered to be an illegal activity. Good to mention that in October 2012, the European Central Bank, was concerned about the growth of the virtual coins, such as bitcoins and Linden Dollar of the online game Second Life. As the ECB was highlighting, this situations could have had a negative impact on the reputation of the Central Banks due to its inherent instability. The Central Banks all around the world observe really carefully the popularity of this virtual coin and its equivalent gaining strength.

5.1.3 "Felonious" Activity

The connections of the bitcoin with criminal activity come to block the attainment of being a widespread credit for basic use and it has attracted the attention of the financial authorities and the legislature. Washington Post refers to bitcoin as "the coin for awful online activities" and CNN named it "the shadowy online credit". USA Senate, New York state and FBI were asked to carefully inspect bitcoin's activity for criminal cases. FBI in 2012 declared that "the bitcoin will continue to attract cyberspace criminals as they use as a way to transfer money and hide funds. Some others believe, for the reasons above, that governments ought to set bitcoins as an illegal ease of credits. More specifically, this allegation comes from professor Steven Strauss of the University of Harvard. Finally, Christopher Tarbell, an FBI Special Agent, said that bitcoins roots are not illegal and there have been many legal transactions, as well. From January 2011 until September 2013,a dark web page named "silk road" used Bitcoins for illegal transactions containing drugs and similars.

5.1.4 Web Security

Until now, most of the web security issues are solved within a few minutes and barely cause problems. The last 4 years of internet use, more possible attack cases have been observed and the security measures are even more strong. Every user can suggest a solution to every matter that he maybe faces and as the Internet grows and the problems are getting more and more, this can be really helpful for a more secure and safe internet browsing, using and online paying. Another problem that concerns the Internet Security world is the infringement of the encrypted algorithms which are a way of securing the web along with other protocols. Their weaknesses were noticed through the years, and most of them can be pretended and the security is largely obtained. The risk is always a matter and as far as the bitcoin is concerned, it needs a while of use in order for their risks to be noticed.

5.1.5 Unclear Legal Framework

Beside the fact that the European Legislation has taken strict measures for all virtual coins, even more parameters are introduced through the years. In Germany, bitcoins are defined as "private money" and in Holland as a credit that does not need control from the Central Bank. In the USA, the only ease of control is to secure its use, which means that they only try to avoid illegal activity and use. It seems to be impossible to completely avoid or forbid every activity that includes bitcoins, and something like that would be extremely difficult to be accomplished.

5.1.6 Fluctuation Rate

The same as every other coin, bitcoin’s value is a matter of offer and demand and is influenced by the range of equivalence. A factor that influences that, is the “small” markets, as the big amount of bitcoin use reflects negatively the equivalence and another one is the kind of the coin as large amounts of “money” can be transferred within a few minutes and it causes critical changes in offer and demand. And at last but not least, the speculative pressures is another factor, as they still have low liquidity and transaction volume.

5.1.7 High Energy Consumption

In order for the mining of this crypto-coin to be accomplished, processing power is needed. In the beginning, through the mining procedure, the central processor of computer was used. They soon noticed that this processor was way slower than the graphics processor and they started using the Graphic Processors for the Bitcoin Mining. Although, high-tech graphic processors have high energy consumption and they cause problems to victualling procedure.

5.1.8 Forbidden usage

Bitcoin’s reputation has faced a lot of problems and banks are hesitant. The coin is gaining acceptance in China and USA but this doesn’t happen in Europe as well. More specifically, the European Bank Principle has already broadcasted an announcement with all the risks and is working on ways of protection. Also, notices the users that every investment on virtual coin can be fatal and they may lose part of their fund. Rumors for interruption of the bitcoin use, proved to be groundless.

5.2 The benefits of Bitcoin

5.2.1 Transparency for transaction and transaction rules

All transactions that have ever been executed in the network are publicly available and transparent. Everyone who wants, now can check an address and see all the past transactions that have been recorded on it, the amount of bitcoins transferred and where they have been transferred to. This can be applied to all transactions that have happened on the network, even on the first one. There is no “secret rule” inside the code of the system and there can’t be one since it’s users wouldn’t accept it.

5.2.2 Privacy of transactions

Every user can create an unlimited amount of addresses and create their transactions through them. Those are private and can’t be traced to the original owner’s address or real information even though they can be identified with real address characteristics so they can be found on the network. This way a user will be able to keep his privacy safe, distinguishing his transactions from his personal information. This doesn’t guarantee complete anonymity for the transactions since all of them are public and if one has public recipient, more information can be extracted for the sender. This is the primary reason that the use of bitcoins is not suitable for illegal transactions, especially for high volumes since the trail of the transactions not only is not deleted but it remains there for everyone to be examined and analysed for ever.

5.2.3 Control from the user

Since the user is the only one who can create and issue a transaction, it is impossible for their bitcoins to be stolen by a third party since the bitcoin encryption has never been decrypted. Furthermore, transaction capabilities under certain circumstances can allow two parties to exchange bitcoins only in specific locations or only after a certain amount of time.

5.2.4 Extremely low transaction costs

The cost of every bitcoin transaction is not dependent on the volume and is extremely low. At the moment the cost of a bitcoin transaction is estimated to be 5 cents and is voluntary if there’s no rush for the transaction to happen immediately. This amount is being given automatically to the users who verify the transaction, as a reward for the processing power they invest to help the network from attacks.

5.2.5 Transaction speed and their intentional nature.

Transactions in bitcoins are immediately announced and issued in the whole network across the globe. This doesn’t require more infrastructure other than the free computer software and internet connectivity.

5.2.6 Consensual use of network

Every change of a characteristic of the network or network rules will be applied only when the community accepts it. That way malign transactions that could change the nature of the network at its core can be avoided since the majority of the users will identify and disallow them. The existence of a technical global community that handles with professionalism the quality of the network while at the same time stays open for comments and changes is the most valuable asset of the network for it’s survival.

5.2.7 Decentralised nature of the network

One of the most important characteristics of the network is its decentralised nature. There is no central authority for transaction validation and every node on the network helps it stay that way. Even if a big amount of nodes gets compromised, that wouldn’t affect the whole network’s use. The only way for the bitcoin network to stop functioning, would be for all the nodes to get disconnected from one another or in other words lose connectivity to the internet, something that is currently not possible. Even in that situation, when the internet starts working again, it will continue after the exact time it stopped, so the blockchain won’t be affected at all.

5.2.8 Subdivisions

Every Bitcoin can be subdivided into up to 8 decimal points (up to 0,00000001). The nature of bitcoin can facilitate micro-transactions that are not feasible with physical coins. The addition of more decimals can be facilitated by the acceptance of this action from the network.

5.2.9 Non reversible nature of the network

All bitcoin transactions are non-reversible. This is an advantage to people who offer an exchange of products for bitcoins since the funds can’t be removed after the transaction happens (something common with credit cards). This gives one more incentive to companies to start accepting bitcoins. This doesn’t mean that the users who are doing bitcoin transactions shouldn't be careful with their choices since a vendor who doesn’t have a solid history of transactions can be something else other than what it looks.

5.2.10 Crisis-resistant

The monetary crisis that we live in, not on hurt bitcoin but at the same time, had a positive turn on its value. The media attention, even sometimes negative, makes even more people aware of it and it now is one of the very few coins that can withstand the pressure of our economy.

Conclusions

The Bitcoin is nothing new.Although known as "money of chaskers" and for money laundering.Is becoming greater than the popularity with many shops to accept as an alternative means of payment.The popularity which takes however could be considered motive for more confidence in this new model money.No doubt the bitcoin presenting a risk but it must also recognize that the bitcoin has played a large role in countries where citizens are facing high taxes on movement of capital.For this if one makes for example the Chinese and the relationship with the bitcoin for which published many articles there is a growing demand for bitcoins. So to date of acceptance by the general public but also academics shows that the project is viable.You could reach up to create the ideal financial system without intermediaries bankers and moneylenders. If that carry out the banks will be reduced to an auxiliary role as international trade foreign exchange and favorable loans.Good is to say that the erroneous use of bitcoin can not destroy the future of the network.Discredits the course but this problem is not inherent in bitcoin but in a way that people choose to use it. They studied all the risks associated with bitcoin but also the positive points of the prospects of concluding network that has much to offer yet.

Bibliography

Daniel Forrester, Mark Solomon, "Bitcoin Explained: Today's Complete Guide to Tomorrow's Currency"

Andreas M. Antonopoulos, “Mastering Bitcoin: Unlocking digital crypto-currencies”

Pedro Franco, "Understanding Bitcoin: Cryptography, Engineering and Economics"

Conrad Barski, Chris Wilmer, "Bitcoin for the Befuddled"

Sam Patterson, Bitcoin Beginner A Step By Step Guide To Buying, Selling And Investing In Bitcoins

A.H. Smithers “Everything you need to know about buying, selling and investing in Bitcoin” Benjamin Guttmann “The Bitcoin Bible Paperback”

Brett Combs “Bitcoin Decoded: Bitcoin Beginner's Guide to Mining and the Strategies to Make Money with Cryptocurrencies”

Marc A. Carignan “The Bitcoin Tutor: Unlocking the Secrets of Bitcoin”
Jose Pagliery “Bitcoin: And the Future of Money”

Paul Vigna “The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order”

Melanie Swan “Blockchain: Blueprint for a New Economy”

Brian Kelly “The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World”