ieee.es
Instituto Español de Estudios Estratégicos

Analysis
Document

13/2014 19th February 2014

David Ramírez Morán

FUNDAMENTALS OF VIRTUAL CURRENCIES: BITCOIN

This document has been translated by a Translation and Interpreting Degree student doing work experience, ALEJANDRA CUBERO ECHEVERRÍA, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.

FUNDAMENTALS OF VIRTUAL CURRENCIES: BITCOIN

Abstract:

Virtual currencies are experiencing a growth in popularity as a result of the constant advertisement they are receiving continuous media publications on the subject. Anonymity's benefits as well as increasing financial interests around this type of actives is having as a result an increase in the number of users and the price in the market. This brief analyses the working fundamentals of one of the most popular virtual currencies: the Bitcoin.

Key words:

Virtual currency, Bitcoin, anonymity, electronic transactions

The virtual money phenomenon is expanding to provide support to activities that take place in cyberspace. One of the first virtual activities that included the virtual currency concept was SecondLife, a social network where users could interact between them in the virtual world that was presented. Users could acquire objects and virtual belongings through the implementation of a virtual currency, the Linden Dollar. In order to obtain credit, users could perform different activities in the game or exchange real money for money in the virtual world. This was the first step in the creation of virtual products for which users were actually willing to pay. This model quickly gained popularity, and new online multiplayer games, where players could obtain objects, missions or upgrades through credit, started to appear.

As a consequence of the Internet boom, virtual paying methods have become the norm to facilitate operations and to gain more security in transactions. The goal is to reduce the risks that encompass the transfer of personal banking data to someone we don't know. Consequently, services like PayPal or Google Wallet, among others, make up a virtual wallet that allows payments in numerous services offered online.

However, there are certain environments where it has been crucial to take a step further in order to attain complete anonymity in the transactions. It is in this context, where anonymity is absolutely essential to complete certain activities, where virtual currencies appear. Virtual currencies do not identify the owner and there is no proof of the operations made, which is why virtual currencies are considered equivalent to cash.

Among these currencies the Bitcoin stands out for its increasing popularity due to its apparition on the media and the capitalization that it has reached in the past months. In the following lines, we will describe the main working principles of this virtual currency in order to, in a following document, analyse the evolution, risks and vulnerabilities that affect the system.

ORIGIN

The Bitcoin is associated with programmer Satoshi Nakamoto, who in 2009 published a document that described how the currency [1]works. He is also linked to the creation of the first application to operate on Bitcoins. However, there are doubts surrounding the nationality and even the real existence of this person, as well as multiple speculations on his real identity.

The Bitcoin consists of a distributed system where there is no central management and which is based on a peer to peer (p2p) where all the nodes may contribute to the working of the system. Initially, all the nodes perform the double function of making the transactions and processing them. However, with the expansion of its use, new applications appeared

[11] Satoshi Nakamoto "Bitcoin; an electronic peer-to-per cash system." Httos://www.bitcoin.org/bitcoin.pdf (consultado el 18/02/2014)

which only allow transaction making, while processing is concentrating on specific systems.

Since it started to run in 2009, the system has gained popularity for the anonymity it provides and the speculative interests that have triggered the evolution of its exchange-rate value to real money.

FUNDAMENTALS

In order for the Bitcoin to fulfil its purpose, it is necessary to be able to make transactions, therefore, there needs to be something to be exchange and it is necessary to identify the parties that are involved in the transactions. The element to exchange is the Bitcoin balance, while the parts are identified through user identifiers. Plus, users must be able to access procedures through which they can carry out operations and know the balance that they have.

BITCOIN AND SECURITY

Bitcoin security is based in the use of cryptography techniques for the protection of the user's balance. The signature and verification of the transaction requests is done through cryptography techniques with public password.

This technique consists of providing a user with two passwords, one named public and the other one private. Currently, knowing one of the passwords does not provide the value of the other one; this way, even if the public password is publicly distributed, a third part will not be able to deduce, obtain or calculate the value of the private password. In order to make operations it is necessary to distribute the public password generally, so when information is forwarded to a user he/she can verify that the information is valid, correct and that matches the information that can only have been generated by a person that has the private password. This is why it is vital to keep in a safe place the private password; all the information that has been signed with a private password will be considered as valid and correct.

The process by which the private password is applied to the information that will be transferred is called signature and consists of acquiring of a number that depends on the information that has to be transferred and the private password. The receptor, on the basis of the information received and the private password of the user, obtains a new number that, if it matches the one sent, allows the validation of the authenticity and reliability of the information.

Once the user's balance security is guaranteed, the system must also assure that the transactions are correct and that a balance owner can't spend it more than once. In order to do so, time stamps, which register the exact moment in which Bitcoin transactions are

requested, are used. The processed nodes take into a count these values to determine when a transaction is valid or not.

BITCOIN IDENTIFIER

A Bitcoin user is assigned an address made up of a 27 to 34 alphanumeric characters chain which starts either by 1 or 3, and which includes several characters, like the control digit of current accounts or de ID letter, that make it possible to verify that the address is correct in order to avoid errors in the typing. This value is equivalent to an account number or a telephone number and clearly identifies the user. The chain contains the information on the public password of the user, which allows the validation of the transactions signed through the private password of this user when they reach one of the network's node.

The conferment of a Bitcoin identifier is free and can be done in new online services as well as in the electronic purses that users are using. A modern computer allows a user to obtain several thousands of identifiers through their assigned passwords in a matter of minutes.

BITCOIN ELECTRONIC PURSE

A Bitcoin wallet is an application, frequently named client Bitcoin, which allows the user to make operations. The application can be on the user's computer, on his phone or in one of the multiple services that are appearing online and which host the user's electronic purse.

The electronic purse manages the user identifiers and its passwords.

Through the application, the user can check the Bitcoin balance in each of its identities and order transactions. Once the sender, recipient and amount values are introduced, the application signs the transaction request and sends it to the mining nodes, which will be described in the upcoming lines.

Block chain

The central core of the Bitcoin is the block chain, which is a list of all the operations that are made using Bitcoins up to date that are validated. It is a file that, as time passes and transactions are added, gets longer.

The balance of a user can only be determined through the block chain. In order to do so, the block chain must be explored, up until the last transaction validated by that identifier.

The block chain is one of the most debated aspects surrounding the anonymity of the system; the information of almost every single transaction is kept without any type of encryption and it is accessible for all users.

Transactions

The necessary information to complete a transaction or to exchange Bitcoins between two or more people is made up of the identifier of the sender, or senders, the recipient, or recipients, the identifiers and the amount, or amounts, of the transaction in the moment when it is ordered.

When a user wants to make a transaction, a request with that information and the signature with his/her private password is generated. This information is sent to all the nodes that deal with them and, after a certain time, this information is incorporated in the block chain permanently. From that moment on, the recipient can check how the balance that is associated to its identifier has increased while the senders will have decreased.

Acquiring Bitcoins

The mechanisms through which Bitcoins can be obtained are several:

- Buying in exchange services that are appearing online.
- Exchange between private individuals.
- Compensation for the selling of products or services.
- Bitcoin mining.

Online intermediaries are appearing; they favour a common exchange point for demand and supply. These services are very important because they are the link to real economy. They allow the acquisition of Bitcoins for money and, most importantly, Bitcoins can be exchanged for cash. These operations are subject to a commission for the one offering the service.

An individual can also exchange without having to look for a specific service. They only need to know the recipient of the transaction identifier and make the order through their Bitcoin purse. In return they can receive money, services or any other benefit that both parts may have agreed, as if it was cash.

Companies are also using the Bitcoin as a paying method for services. The type of business that started accepting payments with Bitcoins was related to illicit activities such as arms, drugs, etc. However, the real economy is also starting to count it in as a valid payment method and there is even a traveling agency that allows the use of Bitcoins[2].

[2] "Los primeros turistas del mundo en comprar viajes con "bitcoins" Diario ABC 30/01/2014. http://www.abc.es/viajar/20140130/abci-turistas-bitcoins-201401291903.html

In order to boost that users actively cooperate in the use of the system, the cooperation in transaction processing is a paid activity that allows the person that provides his/her resources and infrastructures obtain profit from the necessary operations to incorporate transactions to the block chain. This processing, named mining, is a mechanism relatively complex that is dealt with in the following lines.

BITCOIN MINING

Mining is a fundamental mechanism in the functioning of this virtual currency. This is the name given to the procedure by which transactions are incorporated to the block chain and it is key to transaction making. At the same time, it is a unique mechanism through which new Bitcoins are put into circulation.

The term mining is used because it resembles the task undertaken in a gold mine, where a piece of the precious metal is gained for every work hour.

Bitcoin mining can be compared to grocery shopping when prices are unknown. The miner's job is to find an additional product in the shop that, added to a cart of unknown value, makes the final number of zeros in the total amount equal or over a certain number. This operation is complicated because obtaining the total amount is a task that requires a series of operations with each product's price, and this operation has to be redone each time that the additional product does not provide the correct result and, therefore, a new one has to be tried.

The shopping cart would be the equivalent to what in Bitcoin is known as "block"; the products included in the cart are the new Bitcoin transactions between users, and, the product added by the miner to obtain the total amount is known as "nonce", which is nothing more than a number that is added to transaction data and that alters the result if it is raised or varied. Technically, calculating the cart's total amount is, in reality, an operation of double hashing SHA256 in chain, which, from an arbitrary length value sequence gives a 256 bits result, known as 'hash', which has to be lower to a certain threshold.

Obtaining the hash value from the data sequence is a relatively easy operation. However, the opposite operation, which consists of determining the data that a certain hash value produces, is very complex; this is why it is not possible to analytically define the necessary value of "nonce" to validate the block and it has to be done through trial and error.

The first user that is able to find the "nonce" that gives the desired result lets the rest of the network know so the black chain can be updated and it is given a reward for finding the coincidence. From this moment onwards all the transactions included in that block are consolidated in the Bitcoin information chain and, from then on, the rest of the miners that were testing with the data in those blocks have to empty their carts of all the processed products and fill it up with the result of the latest block and the new transactions made by

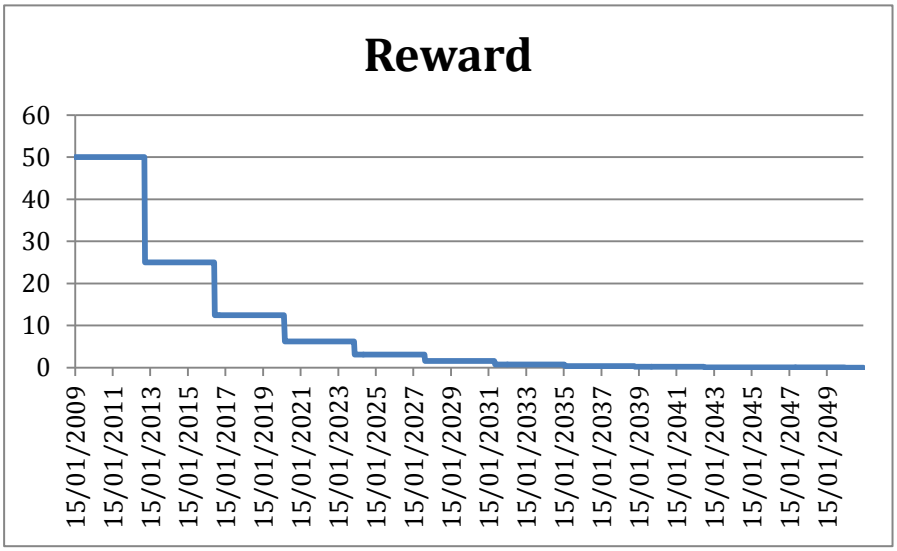
users.

There is a chance that two users obtain a solution simultaneously. Each user's cart will have a different number of transactions, so the Bitcoin infrastructure will only reward the user that has included a large number in his/her cart. This way miners are encouraged to incorporate new transactions regularly, because, if they keep calculating the same products for long, another miner might find a solution that includes more transactions to the ones that already exist.

The difficulty of mining can be adjusted by modifying the threshold that has to be satisfied. The smaller the hash validation threshold, the lower the number of correct "nonce" values, and, in turn, a larger number of different values has to be tried in order to find a valid one. Through the adjustment of the value it is possible to control the speed at which blocks are validated. This value is adjusted so that it validates a block every 10 minutes and the threshold value is corrected every 2160 blocks, which is the equivalent to 15 days.

The time spent until a miner is able to validate a block determines the speed at which Bitcoin transactions can be made. A transaction is not completed until a block that includes is not validated and incorporated to the block chain.

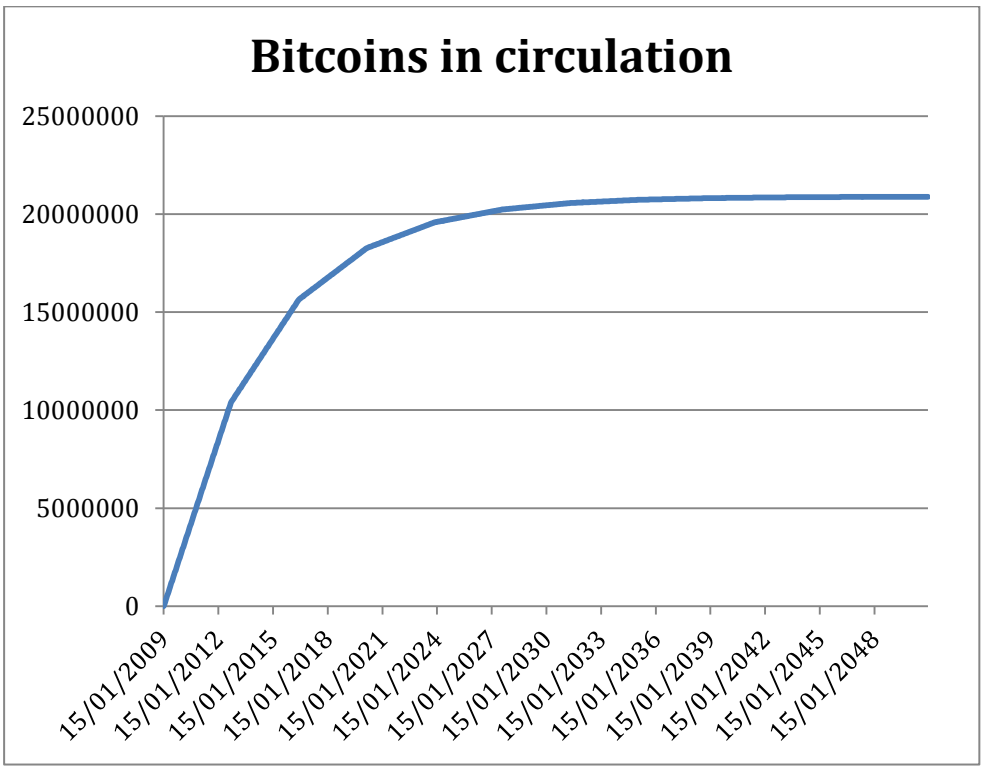
Mining rewarding consists of giving the user that finds the solution to a block a certain amount of Bitcoins. Initially, this amount was of 50 Bitcoins, but the system is contemplating the reduction of this quantity to half every time 210000 blocks are added to the chain. At the moment the reward is established at 25 Bitcoins and, as graph number 1 illustrates, it will lower with time.



Graph 1 – Evolution of mining reward (Source: own development)

Apart from the reward associated to data mining, users can also pay miners to prioritize the inclusion of their operations in the mining process. In fact, as rewards shrink, the payment for transaction will have to be generalized to cover the associated costs to the necessary operation to incorporate new blocks to the chains.

The given rewards for mining tasks are the only procedure by which the amount of Bitcoins in circulation increases. The algorithm in which the functioning is based on poses a limit to the maximum quantity of Bitcoins in circulation, which tends asymptotically to 21 million units (approx.), as shown in graph 2. This value corresponds to the sum of all the rewards that are going to be assigned as transaction blocks are incorporated to the chain. The actual number of Bitcoins in circulation is around 12 and a half millions.



Graph 2 – Evolution in the number of Bitcoins in circulation

VALUE

As there is no institution that backs the Bitcoin value, the price comes exclusively from the price users are willing to exchange it for. The exchange rate is being determined from the operations that are being made in the services that allow the acquisition or selling of Bitcoins and therefore, turn them into cash in any other coin.

It is possible to obtain from the value the total capitalization, which is the result of multiplying the number of Bitcoins in circulation by its value, and it reaches 3750 millions of euros approximately (as of 02/18/2014), even though it topped at 12,500 millions of euros when its value was above 1000€.

ANONYMITY

Once we have the equivalent to cash online, there is only one more step to gain complete anonymity in virtual transactions: eliminating the relation between the Bitcoin identifier and the IP direction of the computer from where the user makes the operations. In order to make a transaction the user has to send the operation data to the nodes that support the Bitcoin. Through the use of "anonymity" technologies, like TOR[3] it is possible to hide the IP direction from which a transaction is being made, which makes it the only method that allows the identification of the person or organization that is using it. This practice establishes and strengthens the relation between the Bitcoin and the deep web.

Another way of contributing to anonymity in the transactions is transferring the sender's entire amount in a single transaction. The agreed amount is sent to the desired addressee, while the rest of the amount is given to a new identifier created by the sender. This way, the original identifier of the sender is left with no balance and can stop using it without a problem. This practice is recommended to favour a regular renovation of user's signature keys, given that for the creation of a new identifier, new keys are created, fulfilling the general recommendation on passwords.

'Tumbling' is a frequent practice among Bitcoin users which consists of transaction making between a big number of different identifiers with amounts that vary to increase the difficulty of finding the path followed by the balance of Bitcoins. For example, from an account of origin the balance is distributed between more accounts with different amounts. At the same time, the amount of those accounts is gathered and separated with different amounts through multiple consecutive operations.

In the last two cases all operations are registered in the block chain so, with the right resources, it would be possible to disentangle these operations.

CONCLUSION

Virtual currencies are increasing their popularity because of the anonymity that allows users to make their transactions. Because of its popularization, new risks in the use of these currencies are appearing.

As any asset that gains popularity and sheds interest on it, new fraudulent practices, that can damage its actual functioning and the interest of those persons who use these types of

[3] Luis de Salvador, REDES DE ANONIMIZACIÓN EN INTERNET: CÓMO FUNCIONAN Y CUÁLES SON SUS LÍMITES. Documento de Opinión 16/2012. Instituto Español de Estudios Estratégicos http://www.ieee.es/Galerias/fichero/docs_opinion/2012/DIEEEO16-2012_RedesAnonimizacionInternet_LdeSalvador.pdf (02/18/2014)

virtual currencies, are appearing.

The increase in the difficulty to obtain Bitcoins through formal procedures is creating multiple techniques to get hold of someone else's Bitcoins. As any system based on new technologies and internet it is subject to attacks which origin is hard to establish and which might have serious consequences in a small space of time, in this case, for users.

States are not unaware of the progress virtual currencies are making, and they are starting to take decisions to regulate its use and its functioning.

The risks and vulnerabilities of these types of virtual currencies, as well as the regulation that is being developed with regards to these initiatives will be dealt with, in detail, in a future analysis.

David Ramírez Morán
IEEE Analyst