

BITCOIN

A Cryptographic currency

INTECO
Instituto Nacional de Tecnologías de la Comunicación
www.inteco.es
@intecocert

CONTENTS

CONTENTS 2
SUMMARY 4
BITCOIN: AN OVERVIEW 6
ORIGINS 6
The creator 8
A NEW PHILOSOPHY 8
CURRENT USE AND ACCEPTANCE 9
Controversy 11
Silk Road 11
Economic considerations 11
Other problems 14
PARTICIPANTS 15
GENERAL CONCEPTS 16
Bitcoin addresses 16
Wallets 16
Transactions 16
Blocks 16
Blockchain 16
Mining 16
OTHER ELECTONIC TRADE SYSTEMS 17
SYSTEMS AND PROTOCOLS 19
CRYPTOGRAPHIC CONCEPTS 19
Digital signatures 19
Cryptographic hashes 19
Random numbers and *nonces* 19
Proofs-of-work 20
THE ARCHITECTURE OF THE SYSTEM 20
DATA STRUCTURES 21
Addresses and wallets 21
Transactions 21
Blocks 23
The blockchain 24
PROTOCOL 25
The first step: the genesis block 25
The process of a transaction 26
Mining a new block 29
Rewards 31

Confirmation of a transaction....32
ANONYMITY AND PRIVACY IN BITCOIN....35
Tracing Bitcoin users....36
Tracing based on analysis of traffic....36
Tracing based on heuristics....36
Mixing services....38
CONCLUSIONS: STRENGTHS AND WEAKNESSES....39
STRENGTHS....39
Distributed trust....39
Incentives....39
Cryptography....39
Scalability....39
Transparency....40
WEAKNESSES....40
Vulnerabilities....40
Theft from wallets....40
Unencrypted traffic....40
Energy Consumption....41
Anonymity and privacy....41
REFERENCES....42
CITED ARTICLES....42
OTHER REFERENCES....42
LIST OF FIGURES AND TABLES....44
FIGURES....44
TABLES....44
APPENDIX I – MERKLE TREES....45
APPENDIX II – SUMMARY OF VULNERABILITIES....47

AUTHORS

Jesus Diaz Vico

Antonio Sánchez Aragó

COORDINATION

Elena García Díez

1 SUMMARY

Under the title “BITCOIN: A Cryptographic currency”, this publication undertakes a technical analysis of the architecture and operation of the Bitcoin digital currency motivated by the interest it holds for the computer security community, given that it is a practical implementation of different cryptographic primitives. Hence, this document does not include recommendations of any type, being the only non-functional content related to the current usage Bitcoin receives at this moment and its acceptance, intended only to provide the necessary context.

The digital currency Bitcoin emerged from the idea of decentralising payments between users, thus eliminating the need for the presence of financial institutions to carry out transactions. Although controversial, in practice it has demonstrated itself to be a workable and valid way of realising transactions and its use is growing worldwide.

Owing to its decentralised nature, Bitcoin was conceived as a peer-to-peer network with records of transactions which could only be altered through impractically complex mathematical calculations.

In order to understand how it works, in addition to knowing the processes by which transactions are carried out and verified, it is also necessary to understand the theory on which it operates and the technology used in its implementation, in order to know how does it achieve security and how to evaluate it.

This document begins with a general discussion of Bitcoin, the most important events in its history, an account of its more controversial features, and an outline of the principal components of the system and how they work. This is followed by a section introducing the cryptographic primitives and data structures on which the system is built, and which analyses in detail the working of the Bitcoin system. This section sets out the process of a transaction, its incorporation into the history of transactions (the ‘blockchain’) and the rewards accruing to those users who dedicate resources in verifying it. Following this, the characteristics of Bitcoin in terms of privacy and anonymity are summarised.

The document ends by setting out Bitcoin’s most important strengths and weaknesses. In anticipation, we can summarise its **strengths** as:

- The system of incentives involved in the operation of Bitcoin, which, in the form of monetary rewards, is key in encouraging the participation of users who act as nodes carrying out necessary complex calculations.
- Bitcoin’s level of security is high, given that it is based on cryptographic primitives of demonstrated security. In addition, its architecture avoids fraudulent practices, such as “double-spending” or unwarranted changes in the system’s operational policies.
- The scalability built into the system’s design and functioning means that its medium and long term operation is guaranteed.
- Given that anyone can see where any bitcoin has come from, and where it goes, Bitcoin is a system which is transparent in nature.

Its **weaknesses** can be summarised as follows:

- Although the network itself is secure by design, its functioning requires certain elements whose definition and operation lie outside the actual network. For example, the security of

the wallets where users store their bitcoins depends on a given user's own knowledge of security.

- All inter-user communications are unencrypted.
- Given that Bitcoin is entirely based on information systems (there is no physical currency), its operation is exposed to possible programming errors and malicious exploitation of vulnerabilities.
- The existence of mechanisms independent of the system by means of which anonymity may be reduced along with the system's transparency, can threaten its users' privacy.
- Given that, by nature, Bitcoin is a system completely dependent on the consumption of energy necessary to carry out the complex calculations required for its operation, participation in it supposes a cost to the users which in the long run may outweigh its benefits.

2 BITCOIN: AN OVERVIEW[1]

Bitcoin is an electronic currency, a protocol and a software. The combined operation of these elements allows the realisation worldwide of near instantaneous peer-to-peer transactions, and consequently payments with low, or even zero, transaction processing costs.

In order to avoid dependence on a central monetary authority charged with the emission and control of currency, Bitcoin functions through peer-to-peer technology. In this system, it is not possible to manipulate the value of bitcoins or produce inflation through the overproduction of currency. Transactions and the creation of bitcoins are governed by the network itself; the creation of money in a controlled and decentralised manner through the process known as 'mining'.

The security of transactions is guaranteed through the use of cryptography. Bitcoins can only be spent by their owner, and they can only be used in a single transaction. The supervision and control institutions that operate in traditional monetary systems do not exist for Bitcoin.

ORIGINS

Bitcoin's first public appearance took place on the *cryptography* mailing list[2], where a user under the pseudonym "Satoshi Nakamoto" posted that he had been working on a new electronic cash system, and summarised its properties by referencing a paper, available on the Bitcoin website (http://www.bitcoin.org), in which he described the system (see Figure 1 1).

Figure 1. "Satoshi Nakamoto's" post to the cryptography mailing list.



Source: The Mail Archive

[1] In what follows here, as in accepted practice, Bitcoin (with an initial capital B) refers to the overall system, and bitcoin (with an initial lower-case b) to refer to the system's digital units of currency.

[2] https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

On 11 February 2009 a user with a profile also under the name of "Satoshi Nakamoto" posted a message on the P2Pfoundation website under the heading "Bitcoin open source implementation of P2P currency"[3] (see Figure 2). In the text of the message, "Satoshi" announced Bitcoin's official website, the system's main characteristics, the paper in which its design was laid out, and even where the first version of the client through which one could participate in the network could be downloaded.

Figure 2. "Satoshi Nakamoto's" message on the P2Pfoundation.



Source: P2Pfoundation.

[3] http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

The creator

Up to now, the identity of the creator, or creators, of Bitcoin is unknown. “Satoshi Nakamoto” is the pseudonym used by the person or group of people who designed and built the Bitcoin network in order to maintain their anonymity and protect themselves and the network.

All that is known about “Satoshi Nakamoto” is contained in his profile on the *P2Pfoundation* site, according to which he was (at the time of writing) a 38-year-old Japanese male. However, it is obviously not possible to ascertain that this information is accurate or true at all. Nevertheless, given the design of Bitcoin, it can be said that its creator(s) would have to have an advanced level of expertise in cryptography and mathematical algorithms.

There has been a great deal of speculation about the real identity of “Satoshi Nakamoto”. Some have pointed to Shinichi Mochizuki, a mathematician specialising in number theory and a professor at the University of Kyoto. Others have suggested that behind “Nakamoto” lie figures related to black markets and criminal networks.

In 2011, by means of an email to one of Bitcoin’s developers, “Satoshi Nakamoto” disassociated himself from the project, and announced he was dedicating himself to other matters.

A NEW PHILOSOPHY

Leaving aside its technical aspects for the moment, Bitcoin is novel because it does not rely on a central authority charged with either creating currency units or verifying transactions. Owing to its distributed architecture, it is the system’s users who implicitly and “democratically” take these global decisions. How the system works can be approximately described through the following two examples:

1. As a reward for collaborating in the network, users receive bitcoins (exactly how, will be seen below). But it is not possible for users to cheat the system in order to increase their rewards, because the system is designed in such a way that it is the users themselves who subsequently have to verify the rewards. In this way, should one user try surreptitiously to increase his or her reward, the rest would not permit it.
2. User *A* makes a payment to user *B* using bitcoin *b1*. To avoid *A* using *b1* to make a payment to a third user *C*, Bitcoin transactions are public. When the rest of the network detects the second transaction, it does not permit it, making it impossible for *A* to reuse *b1* a second time.

It is thus the users themselves who take the decisions normally taken by a central monetary authority. It is this that makes Bitcoin a “democratic” currency. As in any democracy, the evolution of the system is shaped by what the majority of the population wants. There is not, however, an equivalent here to “*one user = one vote*”, since the weight each user enjoys in the system depends on the computing power they dedicate to the network; in Bitcoin it is more the case that “*x% of computing power = x% of votes*”. Thus, as long as more than 50% of the network’s computing power is in the hands of honest users, the network will evolve in the direction that they decide [1, p. 3]. The principle here can be imagined as a “weighted democracy”, determined by the scale of the users’ involvement in the system.

Seen in this way, Bitcoin represents a totally new economic and social scenario. The adoption of Bitcoin, or an equivalent system, would mean that governments and financial authorities would be unable to control the evolution of currency directly. Of course, indirect influence, through legislation, could be exerted, but not control over its behaviour. An electronic currency has an international, rather than national, character: effective legislative

control over it would be a complicated matter. In addition, considering that these scenarios are without precedent in economic theory, the effects of Bitcoin's acceptance and use on a grand scale are unpredictable.

CURRENT USE AND ACCEPTANCE

As has already been noted, this document only deals with a technical analysis of the architecture and functioning of the electronic cash system and not with considerations arising from its use. The summary of its use and acceptance contained here is only intended to give the reader general context. For a wider grasp of the implications of its use, there is a range of materials available from banking authorities, such as the European Banking Authority, which give recommendations regarding the use of virtual currencies.[4]

The number of companies and small businesses who accept Bitcoin as a means of payment is increasing constantly. Currently, Bitcoin can be used to buy a whole range of services, such as telephone services, internet hosting, gift cards, legal advice, tourism, etc. Its rate of adoption can be explained not only by its international reach but also in part by the sense of anonymity that it generates, which has stimulated its use for illegitimate proposes, and in situations in which political pressures prohibit other forms of virtual payments.

Nevertheless, its adoption is not exempt from attempts to exert control over it on the part of governments and regulatory bodies. For example, in mid 2013 the State of California wrote to the Bitcoin Foundation, informing it that if it did not register as a money transmitter it would not be able to operate in that state (see Figure 3), while in December 2013 the People's Bank of China decided to bar financial institutions from handling Bitcoin transactions.[5]

Recently (early 2014), however, Bitcoin received two important endorsements: from February 2014, eBay[6] will allow transactions in Bitcoin (although for the moment only in the United Kingdom), and Google[7] has also confirmed its interest in the currency.

Figure 3. California orders Bitcoin to cease operations.



CNET › News › Internet & Media › Bitcoin Foundation ordered to cease operations in California

Bitcoin Foundation ordered to cease operations in California

Nonprofit organization devoted to promoting the virtual currency is accused of transmitting money without a license.

by Steven Musil | June 23, 2013 5:46 PM PDT

Follow @stevenmusil

The Bitcoin Foundation, a nonprofit devoted to promoting best practices for the virtual currency, has been ordered to cease operations in California.

The California Department of Financial Institutions, which oversees banks, credit unions, and other financial organizations operating in the state, sent a cease-and-desist letter (see below) last month to the foundation accusing it of "engaging in the business of money transmission without a license or proper authorization."

[4] http://www.eba.europa.eu/documents/10180/16136/EBA_2013_01030000_ES_TRA1_Vinay.pdf
[5] http://tecnologia.elpais.com/tecnologia/2013/12/05/actualidad/1386240024_458907.html
[6] http://news.cnet.com/8301-1023_3-57617502-93/ebay-to-allow-bitcoin-sales-in-virtual-currency-category/
[7] http://www.forbes.com/sites/andygreenberg/2014/01/22/google-lets-slip-that-its-exploring-possible-bitcoin-integration-plans/

Source: CNET

In the US, the Department of the Treasury's Financial Crimes Enforcement Network drafted a guide on virtual currencies[8] to close potential legal loopholes. In outline, while the guide accepted these types of currencies (Bitcoin included), it also defined the obligations that their users had to fulfill on realising money transfers and, along these lines, the necessity of registration as a money transmitter. It should be emphasised here that the Bitcoin Foundation does not itself manage money transfers and is therefore not legally obliged to register itself as a money transmitter.

In Spain too, as can be seen in Figure 4 and Figure 5, the use of Bitcoin is on the up and there is now a large number of businesses across the country who accept is as a means of payment for their products and services. The Bitcoin Wiki[9] lists the sites where bitcoins are accepted for services provided through the Internet.

Figure 4. Map of Businesses which accept bitcoins in Spain.



Source: Mercado BITCOIN

Taking advantage of the repercussions that the use of Bitcoin is having on an international scale, adoption of the currency is seen as newsworthy. Thus, given increasing public awareness of the use of Bitcoin in the world of commerce as an alternative to traditional card payment methods, its acceptance has been used as leverage in terms of publicity and visibility.

[8] http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf
[9] https://en.bitcoin.it/wiki/Trade

Figure 5. News report on the use of bitcoins in bars in Spain. Translation: "During financial crisis times, virtual wallets: Spanish pubs join in Bitcoin"



RT Actualidad / Economía

http://es.rt.com/pC8 Imprimir

En tiempos de crisis, monederos virtuales: Bares españoles se suman al uso del bitcóin

Publicado: 26 jun 2013 | 13:33 GMT Última actualización: 26 jun 2013 | 13:33 GMT

0 0 0 ∞ ∞

Corbis

La moneda virtual bitcóin gana popularidad en España. Decenas de restaurantes y bares empiezan a aceptar este tipo de cambio.

El bitcóin comienza a hacerse un hueco en España más allá de Internet, y la moneda virtual ya funciona en la calle. Además de las transacciones electrónicas, decenas de empresas, especialmente bares y restaurantes, aceptan ya los bitcoines.

Todo sobre este tema

Source: RT ¡SEPA MÁS!

Controversy

Aside from the technical aspects, the fact that Bitcoin is a currency outside of state control has made it an object of controversy. On the one hand, there are those who consider it a great tool to limit the control of governments over the popular economy. On the other, it is seen as a source of illegitimate activities (in more or less the same terms as the debate over the Tor network[10]). In addition to this, given the new scenario it supposes, it is also not clear what effects on the global economy the massive adoption of Bitcoin would have.

Silk Road

One of the polemics (at times provoked by an unjustified sensation of anonymity) surrounding Bitcoin arises from the fact that it has been used for illegitimate ends. For example, the Silk Road market[11], closed down by the FBI[12], only accepted payments in bitcoins. When Silk Road was closed down, the FBI seized a part of Ulbricht's Bitcoin fortune (about 144,336 bitcoins) and transferred it to accounts controlled by the FBI, subsequently publicising the identity of these.

Economic considerations

The value of Bitcoin is determined like it is done with other currencies, such as the euro and the dollar. Bitcoin can be seen as fiat money, whose value is based in the trust that society deposits in it. Nevertheless, the fact that Bitcoin is uncontrolled by any authority means that the basis of this trust are different. In the case of official currencies, it is the trust of the state or authority which supports it what determines its value, and which provides it with mechanisms to prevent its value from rising or falling beyond limits considered inadvisable.

10 http://inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/red_tor_anonimato_vulnerabilidades

11 http://www.npr.org/2011/06/12/137138008/silk-road-not-your-fathers-amazon-com

12 http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

In the case of Bitcoin, its exchange rate value[13] with official currencies will rise to the degree that society in general (users, traders, etc.) accepts payments in bitcoins and fall to the degree that it does not.

Because it is a currency different to all those that have previously existed, in addition to being relatively new (with only a few years life), its exchange value fluctuates greatly owing to the fact that the level of trust invested in Bitcoin is not as great as that invested in other official currencies. In addition, this level of trust can be affected by technical factors. To give one example: between 11 and 12 March 2013[14] an update of the database used by the main bitcoin miner software, "bitcoind", produced an inconsistency between versions of the currency. This led to the appearance of two parallel chains of currency (a "fork"). For a period of time, one set of Bitcoin users followed one chain, while the rest followed the other, generating a confusion which led to a depreciation of the currency, illustrated in Figure 6.

Figure 6. The depreciation of Bitcoin during the fork of March 2013.



Nevertheless, owing to the specific construction of Bitcoin, such situations will self-correct over time, through annulling one of the chains, leaving only one valid chain.

The value of bitcoins can also be affected by theft, scams, contingencies (such as the closing down of Silk Road), which can introduce uncertainty and mistrust into the system. Figure 7 shows the effects of two important events of this type which occurred in the life of Bitcoin: the "*Linode hacks*"[15] of March 2012 (above), which saw the theft of approximately 46,653 bitcoins; and the "first" closing down of Silk Road[16] on 2 October 2013 (below), when 144,336 bitcoins were confiscated from its founder.

[13] http://bitcoin.org/en/faq#why-do-bitcoins-have-value
[14] http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/
[15] https://bitcointalk.org/index.php?topic=83794.0#post_linode_hacks
[16] https://bitcointalk.org/index.php?topic=83794.0#post_silk_road_seizure

Figure 7. Effect of the "Linode hacks" (02/03/2012) and the closing down of Silk Road (02/10/2013) on the price of bitcoins.



Decisions taken by governments or large companies can also impact on the value of bitcoins, despite the fact that Bitcoin is not controlled by any state or authority. For example, the decision by the People's Bank of China to bar the handling of Bitcoin transactions[17] had the short-term effect shown in the upper part of Figure 8, and was probably responsible for the medium-term effect shown in the lower part.

[17] http://tecnologia.elpais.com/tecnologia/2013/12/05/actualidad/1386240024_458907.html

Figure 8. The effects of People's Bank of China to bar the handling of Bitcoin transactions.



All this goes to show that the Bitcoin ecosystem is still in its infancy and that contingencies can have greater than expected effects.

In addition to this, much is unknown about the effects of a large-scale adoption of virtual currencies. In 1996, Tatsuo Tanaka, of Columbia University, carried out an analysis of the possible consequences of this under the title "Possible Economic Consequences of Digital Cash"[18]. If we follow his analysis, Bitcoin would now find itself in a phase of "expansion", and the possible phases of "confusion" and "organisation" to come could carry with them significantly uncertain consequences.

Another feature that marks Bitcoin out is, as Paul Krugman has noted, that the fact that the total number of bitcoins permitted is limited to 21 million promotes their accumulation, since their future scarcity will bring about an expectation of a rise in their value[19].

Other problems

In addition to these problems, the fact that Bitcoin is managed electronically opens up new lines of attack for malicious software. Between 31 December 2013 and 3 January 2014, Yahoo experienced a security problem with adverts on its homepage. Some of these were infected with malware which allowed the hidden installation of Bitcoin mining software, creating what was effectively a mining botnet[20]; some experts estimate that this type of

[18] http://www.isoc.org/inet96/proceedings/b1/b1_1.htm
[19] http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/
[20] http://www.bbc.co.uk/news/technology-25653664

botnet is capable of generating $100,000 a day. There have also come to light cases of ransomware[21], in which "ransoms" are demanded in bitcoins, as is the case with Cryptlocker (Figure 9).

Figure 9. Cryptlocker ransom message.



PARTICIPANTS

Of the participants in the Bitcoin system, two not necessarily mutually exclusive groups can be distinguished:

- **Normal users**: users of the Bitcoin system who buy and pay for goods and services with bitcoins, producing transactions in the system.
- **Miners**: special users who dedicate computing power to verify new transactions, creating what are known as transaction blocks. The calculations required to do this are expensive in computing power, which is why these users are rewarded.

In addition to these, there is a third group which is frequently not taken account of: **developers**. Bitcoin's main medium is software and, as such, it requires development and

21 Ransomware (or Cryptovirus): malicious code which makes specific files on a computer inaccessible, and coerces the user to pay a 'ransom' to be able to access the data http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Ransomware

maintenance, for which a team of developers is essential. The current "official" Bitcoin.org client is backed by six developers[22]. Nevertheless, because it is a free protocol, anyone can create a Bitcoin client; and in fact there are various in existence[23].

Despite their apparently central and especially influential position, however, developers are not able to impose decisions on the system. For example, although the developers could decide to increase the reward for the discovery of a new block from, say, 50 to 100 bitcoins, should the majority of users (or rather those who together provide more than half of the computing power) oppose that decision, they would be able to change over to another Bitcoin client which would maintain the reward they considered fair. In the extreme case, anyone can implement their own client as long as this was compatible with the protocol. Thus, although the service provided by the developers is essential, their influence is limited.

GENERAL CONCEPTS

To begin describing the general functioning of the system, here is set out the basic concepts on which the system is based. After this, Figure 10 shows in simple schematic form how a Bitcoin transaction is carried out. Each one of the steps is then explained in greater detail.

Bitcoin addresses

This is a user's virtual address, which contains bitcoins and which is used to make and receive payments, similar to a bank account. A given user can have as many addresses as needed, and they are identified by a public key.

Wallets

A virtual space, equivalent to a physical wallet, where a user's Bitcoin addresses and the payments made with these are stored and managed.

Transactions

A transaction is a transfer of money from Bitcoin address *A* to another address *B*. To create a transaction, the owner of address *A* signs a transcription of address *B* (amongst other data) with the private key associated with address *A*, so that the whole network knows that the new legitimate owner is the owner of address *B*.

Blocks

This is a structure that brings together transactions. Transactions whose confirmation is pending are brought together as a block in a process which is known as mining.

Blockchain

This is the public record of verified Bitcoin transactions in chronological order. When a block has been confirmed, through mining, it is included as part of the chain.

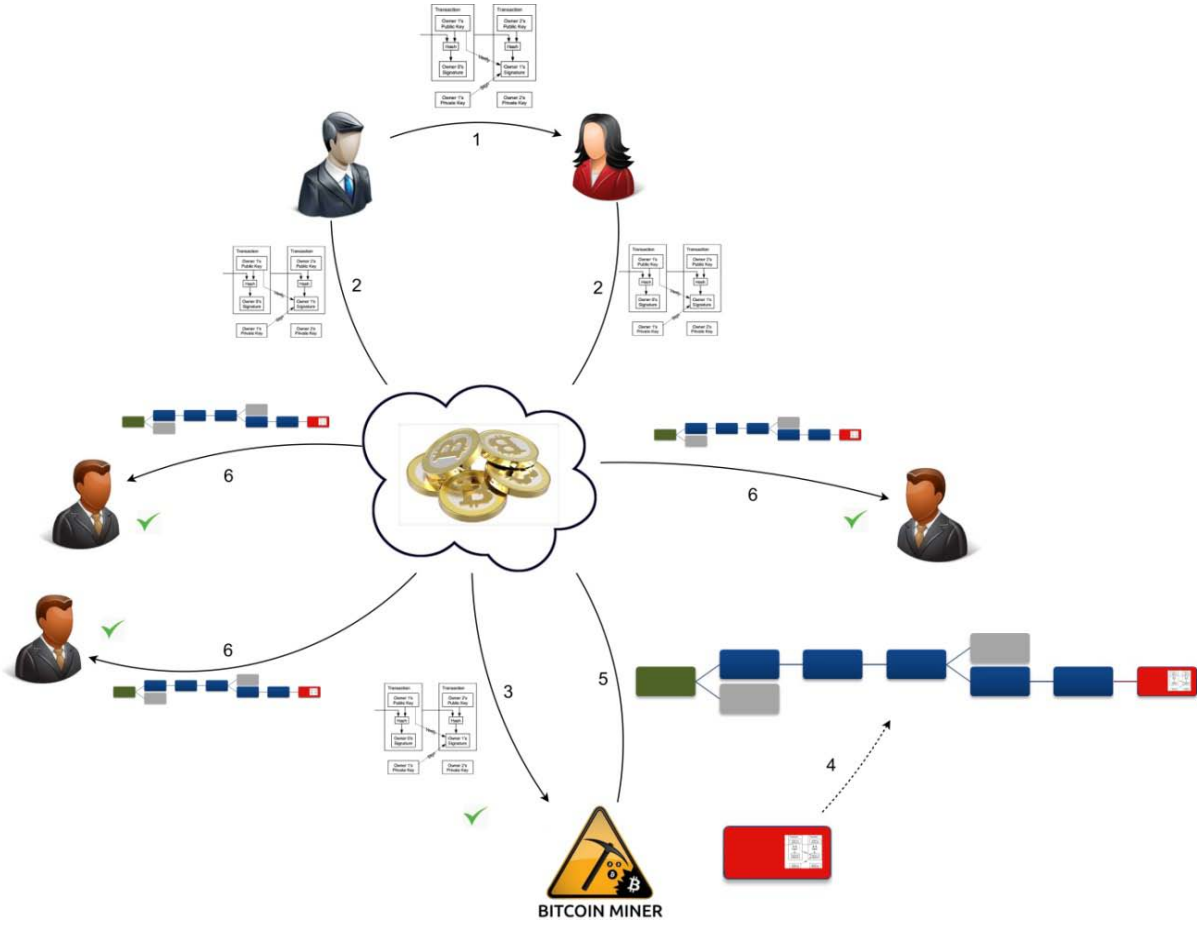
Mining

It is the process of carrying out mathematical calculations in the Bitcoin network. New bitcoins are created through mining as transactions are confirmed.

[22] http://bitcoin.org/en/development

[23] A list can be found here: https://en.bitcoin.it/wiki/Clients.

Figure 10. The generic functioning of Bitcoin.



1. *Bob makes a payment with bitcoins to Alice.*
2. *Both Alice and Bob send the transaction to the Bitcoin peer-to-peer network.*
3. *A miner receives the new transaction and verifies it.*
4. *The miner creates a set of new transactions, including that of step 1, and works to confirm it.*
5. *The miner sends the new block of confirmed transactions to the Bitcoin peer-to-peer network.*
6. *The rest of the Bitcoin users update their status including the transaction block, verifying that the block is valid.*

As can be seen, both normal users and miners participate actively in the system, although it is the latter who carry the greater computational load. It should be emphasised here that there is never any need for the intervention of any authority. If a miner refuses to process a transaction, eventually another miner will. Nowadays, given that the computational power to carry out the verification of transactions is very high, there exist pools of miners – groups who work together to verify the same transaction block and who then share the reward amongst themselves.

OTHER ELECTONIC TRADE SYSTEMS

Even though it is currently the best-known, Bitcoin is not the only electronic cash system; nor is it the first. The idea first appeared in 1985, put forward by David Chaum in the paper

entitled “Security without identification: Transaction systems to make Big Brother obsolete” [3]. Since then, a multitude of systems, incorporating improvements in various aspects, or replacing certain characteristics with others, have been proposed. Testimony to this is the list in Wikipedia[24] of electronic cash systems that operate on a strong cryptographic base (the so-called cryptocurrencies), which includes around 50 electronic cash systems.

Bitcoin stands out here, as has already been noted, because it is the first system which functions without a central authority. All of its activity is “regulated” in a distributed manner. In this aspect Bitcoin has been a pioneer, and, as *The Economist* website pointed out,[25] whatever else happens to Bitcoin, this feature will markedly influence the evolution of any other system.

[24] http://en.wikipedia.org/wiki/List_of_cryptocurrencies
[25] http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital

3 SYSTEMS AND PROTOCOLS

Systems of the complexity of Bitcoin are always backed up by an advanced set of primitives; without knowing the primitives, understanding how a great deal of the properties of the system are achieved is impossible. For this reason, now that the general operation of the system has been set out, this section will look at the system's fundamental primitives in detail.

CRYPTOGRAPHIC CONCEPTS

The cryptographic primitives that Bitcoin makes use of ultimately determine the system's desired security properties.

Digital signatures

Bitcoin uses the ECDSA (Elliptic Curve Digital Signature Algorithm)[26] to sign its transactions, using parameters recommended by the Standards for Efficient Cryptography Group (SECG), secp256k1 [3]. The signatures use DER encoding[27] to package their components into one single flow of bytes.

ECDSA offers advantages over other signature systems which make it ideal to be used for a distributed Internet protocol, namely:

- Short key and signature lengths.
- Rapid generation and verification.

Cryptographic hashes

In the hash calculations carried out in Bitcoin, the SHA-256[28] standards are used, and when shorter hashes are required, RIPEMD-160[29]. Normally the hash calculations are carried out in two phases: the first with SHA-256, and the second, depending on the length desired, with SHA-256 or RIPEMD-160 .

```
SHA-256("Hola") = E6 33 F4 FC 79 BA DE A1 DC 5D B9 70 CF 39 7C
82 48 BA C4 7C C3 AC F9 91 5B A6 0B 5D 76 B0 E8 8F

SHA-256(SHA-256("Hola")) = A7 53 96 6A 11 02 90 57 D6 50 C4 C3
0C 2E 3F 52 8A B6 83 8B 96 C7 BA BB 74 3A EB 9E 3D 6B C4 01

RIPEMD-160(SHA-256("Hola")) = F9 3B 68 56 C7 BD 9F 91 97 F7 B5
0F 35 93 09 EE 98 80 92 41
```

Random numbers and *nonces*

Random numbers and their generation are fundamental pillars of cryptography. Nonces are "special" random numbers, which, in principle, are only used once (hence their name: **n**umber used only **once**), although at times the terms are used indistinguishably.

[26] http://es.wikipedia.org/wiki/ECDSA
[27] http://en.wikipedia.org/wiki/Distinguished_Encoding_Rules
[28] http://es.wikipedia.org/wiki/Secure_Hash_Algorithm
[29] http://es.wikipedia.org/wiki/RIPEMD-160

In Bitcoin, random numbers and nonces are used directly in the formation of blocks. As will be seen, to make a new block, a random number that satisfies certain requirements needs to be found. Random numbers are also indirectly used in Bitcoin as part of the digital signature algorithm (ECDSA).

An example of the importance of this component is the vulnerability[30] detected in August 2013, when a poor initialisation of the random number generator in Android devices allowed the private keys associated with Bitcoin addresses to be deduced (ECDSA[31] insists that the random numbers used in different signatures be themselves different).

Proofs-of-work

Proofs-of-work are the main component guaranteeing the Bitcoin network's legitimate behaviour. In short, the idea is that verifying/calculating new transaction blocks supposes a high computational cost, such that to take control of the network (and hence of what is verified and what is not) an attacker would need a computing power extraordinarily difficult to achieve. The original precursor of this idea is the Hashcash[32] method, devised in 1997 against the sending of spam.

Concretely, this control of complexity in the calculation of new blocks is carried out by requiring that the hash for each new block starts with a given number of zeros. As will be seen, older block data and a nonce are combined to calculate this hash. Given that cryptographic hash functions are not invertible, in order to find a new valid block the only alternative would be to obtain different nonces until one which fulfills the pre-established requirement is found.

THE ARCHITECTURE OF THE SYSTEM

The nodes which integrate Bitcoin comprise a peer-to-peer communication system. As has already been mentioned, the philosophy here is to avoid server roles which could evolve into, or be used by, central authorities, governments, etc.

Like any other peer-to-peer system, Bitcoin encompasses a series of mechanisms to discover new nodes[33] in the network and maintain an up-to-date list of these. In addition, specific Bitcoin clients, such as the Satoshi client[34], can offer additional mechanisms. Among the main options, the *addr* and *getaddr* messages stand out. These allow a client to send to (or solicit from) another a list of clients currently connected to the network. A list of seed nodes is also usually included in the client code. This can be used to start the process of connection to the network, should the other mechanisms fail. In December 2013, the seed nodes included in the "official" Satoshi client were :

- *seed.bitcoin.sipa.be*
- *dnsseed.bluematt.me*
- *dnsseed.bitcoin.dashjr.org*
- *bitseed.xf2.org*

In addition to the mechanisms to find other nodes in the network, there are other types of message frequently used in Bitcoin. For example, the *tx* and *block* messages are used to send respectively transaction data and blocks, so that the nodes in the network are able to

[30] http://bitcoin.org/en/alert/2013-08-11-android
[31] http://en.wikipedia.org/wiki/Elliptic_Curve_DSA#Signature_generation_algorithm
[32] http://en.wikipedia.org/wiki/Hashcash
[33] https://en.bitcoin.it/wiki/Network
[34] https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery

maintain the synchronisation required by the protocol; and messages of the *inv* type, which are used to announce (and retransmit) new transactions.

A complete list of the types of messages, along with their definition and explanation, can be found in the Bitcoin Wiki[35].

DATA STRUCTURES

This section will look at how the system's distinct concepts are built from these cryptographic primitives.

Addresses and wallets

A Bitcoin address is made up of a pair of ECDSA public and private keys. The address is identified by the public key's hash, to which the checksum is added. This is then encoded in a modified version of base 58[36], which maintains the zeros on the left when the encoding is carried out. Thus, an address is identified in the following way:

```
$Version = 1 byte de ceros
$KeyHash = $Version + RIPEMD-160(SHA-256($PublicKey)
$Checksum = SHA-256(SHA-256($KeyHash))[0-3]
$BitcoinAddress = Base58Encode($KeyHash + $Checksum)
```

On being identified by the ECDSA public key, all the operations carried out with this address have to be supported by the use of the associated private key.

Wallets are thus a grouping together of public and private keys.This does not suppose any limit on the wallets being used to carry out other tasks, for example realising transactions.

Transactions

Bitcoin transactions are digitally signed records which change the ownership of Bitcoin funds by assigning them to another address.

A transaction is made up of the following components, forming the structure set out in Figure 11:

- **inputs**: records which reference previous transactions
- and **outputs**: records which determine the new owner of the transferred bitcoins.

The outputs are uses as new inputs for future transactions. In addition, all the bitcoins which are in the output addresses are always used, i.e. the entire sum of outputs cannot be split up even if it is greater than the amount to be paid: should this be the case, another output, by means of which the buyer will receive 'change', is generated.

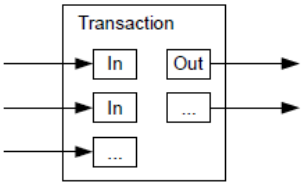
Specifically, a Bitcoin transaction is composed of the fields set out in Table 1[37].

[35] https://en.bitcoin.it/wiki/Protocol_Specification#Message_types
[36] The rationale behind the use of base 58 over base 64 is set out in https://es.bitcoin.it/wiki/Codificaci%C3%B3n_Base58Check
[37] https://en.bitcoin.it/wiki/Transactions

Table 1. Transaction fields.

Field	Description
Version no	Currently 1
In-counter	Number of inputs in the transaction
List of inputs	List of inputs in the transaction
Out-counter	Number of outputs in the transaction
List of outputs	List of outputs in the transaction
Lock_time	The block number or timestamp until when a transaction is blocked.

Figure 11. A transaction.

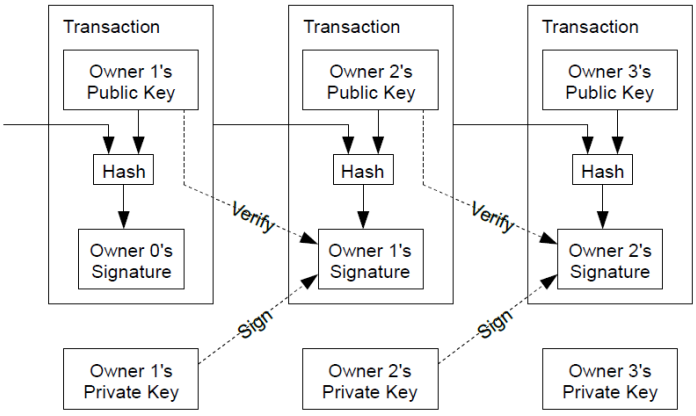


Source: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

Each transaction input is digitally signed by the payer, who unblocks the funds contained in the address associated with the private key used in the signature. In this way, only the owner of the corresponding private key is able to create a valid signature. This, in turn guarantees that only the owner of the money can use it. This process is displayed in Figure 12.

The outputs consist of the address of the payee, and, if necessary, an address owned by the payer to receive change.

Figure 12. Transaction signatures.



Source: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

In a transaction, the sum of inputs has to be equal to or greater than the sum of outputs. In the case of the quantity of bitcoins in the input being greater than in the output, the difference is considered a transaction fee, and whoever includes this transaction in the blockchain can use it. This acts as an incentive for miners, who receive a **reward** for their efforts in the form of bitcoins, it being the payers who normally establish the fee to be included in their payments (although many Bitcoin clients use default values). It is therefore common for transactions with higher fees (i.e. rewards) to be processed more quickly than transactions with lower ones.

There are also special transactions, which are the result of the creation of new bitcoins through mining, for which there are no inputs.

There is a subtle but important difference between Bitcoin and physical monetary systems when it comes to theft. When someone steals physical money, its legitimate owner can no longer use it, given that its physical presence passes into the (illegitimate) ownership of the thief. In the case of Bitcoin, if someone "steals" bitcoins by appropriating the associated private keys, the theft will not be effective until the thief transfers the stolen bitcoins to an account under his ownership (as long as the victim keeps at least one copy of the private keys). Otherwise, given that the legitimate owner obviously knows the associated private keys, he can transfer them to a new account for which the thief does not know the private key, thus preventing the consummation of the robbery.

Blocks

A block is a record which contains confirmations of pending transactions. On average, around every 10 minutes a new block including new transactions is added to the blockchain through mining.

A block is composed of the fields set out in Table 2[38].

Table 2. Block fields.

Field	Description
Magic no	Value always 0xd9b4bef9
Blocksize	The number of bytes that follow up to end of block
Blockheader	Header containing metadata on the block and the chain
Transaction counter	The number of transactions in the following list
Transactions	The list of transactions contained in the block

The list of transactions includes the new transactions that the miner who has calculated the block has decided to include. Which transactions are included is mainly up to the miner. The block header includes the fields set out in Table 3[39].

[38] https://en.bitcoin.it/wiki/Blocks
[39] https://en.bitcoin.it/wiki/Block_hashing_algorithm

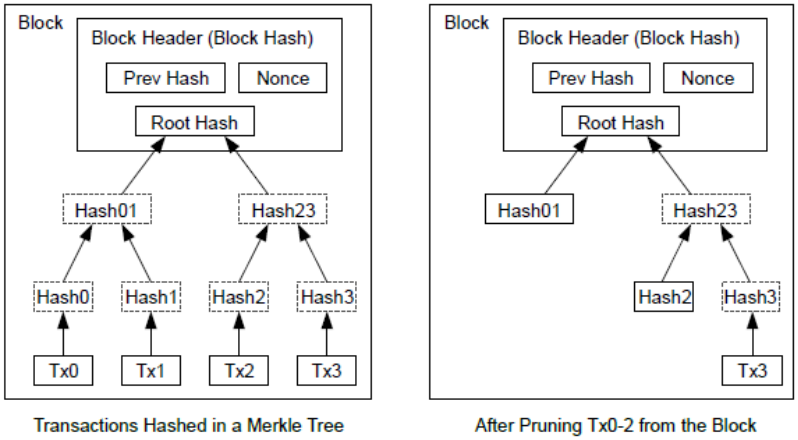
Table 3. Block header.

Field	Description
Version	Block version
hashPrevBlock	Hash of the previous block
hashMerkleRoot	Hash of the Merkle tree root
Time	Block creation timestamp
Bits	Specification of the block's complexity
Nonce	Proof-of-work

- The hashes included in the second and third fields have are aimed to establish the blockchain (which will be looked at below).
- The *bits* field defines the level of complexity required at the moment of the block's generation for each block to be valid. This complexity varies with the overall computing capacity, so that each block is generated, on average, every 10 minutes.
- The *nonce* value is the number that demonstrates proof-of-work. Specifically, proof-of-work consists of calculating the hash (SHA-256) of the six header values; the resulting hash has to be lower than the value encoded in *bits*.

To optimise the disc space necessary to store the blockchain, the transactions included in each block are organised as a Merkle tree (see Figure 13). Given the construction of these trees, a great part of the transactions included in the tree can be eliminated or pruned without compromising the integrity of the block.

Figure 13. Blocks and transaction pruning.



Source: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

The blockchain

The Bitcoin network's blockchain is a collectively created list of all transactions confirmed and verified by the network itself through incorporating transaction blocks.

When a node in the network creates a new block, it sends it to the rest of the nodes. These verify that the block is correct, and if it is, they add it to their chain, and disseminate it. Through this dissemination, the new block ends up being added, provided that another branch in the blockchain has not been created in which a number of users with greater computing capacity have participated.

Given this, by following the list of transactions, the history of the possession of all bitcoins in the system can be obtained from the blockchain. Due to this, a user cannot double spend already used money, since the network itself would block the transaction In the Blockchain site[40], recent cases of money double spending, detected and blocked, can be seen.

It should be noted that bitcoins can also be reused non-maliciously when, for example, large-scale communication failures, such as network disruptions, occur; or when branches in the chain, each containing approximately half the computing power of the system, are created.

For this reason, it is good practice to wait for a given time to confirm a transaction, for the Bitcoin payee to be able to consider the payment actually received. By default, the most widespread clients include a waiting time of six blocks, i.e. until six blocks since that which includes the transaction have been verified, the payment is not considered as effectively performed. Given that the average time for the generation of blocks is one every ten minutes, this supposes that transactions will take around one hour to be confirmed.

Finally, the blockchain, as far as its data structure is concerned, is established through the *hashPrevBlock* and *hashMerkleRoot* fields of each previous block.

PROTOCOL

In this section the functioning of the Bitcoin system will be looked at in some detail, beginning with the first step of the system, the genesis block, and following its operation through a transaction analysed using the concepts outlined above.

The first step: the genesis block

To start the Bitcoin system up, a first block, known as the **genesis block**, was created, with a reward of 50 bitcoins, the first cash in the network.
An interesting fact worth mentioning is that the creator of the block inserted as one of its parameters (the parameter *coinbase*, in lines 30 to 32 in Figure 14, in hexadecimal format) the following message:

> *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*

This text, which makes reference to the cover of The Times diary, was included within the genesis block as a proof that the network begun to function after 3 January, 2009.

[40] https://blockchain.info/double-spends

Figure 14. The genesis block.

```
{
"hash":"0000 0000 0019 d668 9c08 5ae1 6583 1e93 4ff7 63ae 46a2 a6c1 72b3 f1b6
0a8c e26f",
"ver":1,
    "prev_block":"0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
                  0000  0000 0000 0000",
"mrkl_root":"4a5e 1e4b aab8 9f3a 3251 8a88 c31b c87f 618f 7667 3e2c c77a b212
             7b7a fded a33b",
"time":1231006505,
"bits":486604799,
"nonce":2083236893,
"n_tx":1,
"size":285,
"tx":[
  {
  "hash":"4a5e 1e4b aab8 9f3a 3251 8a88 c31b c87f 618f 7667 3e2c c77a b212 7b7a
          fded a33b",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":204,
  "in":[
    {
    "prev_out":{
    "hash":"0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
            0000 0000 0000",
    "n":4294967295
    },
    "coinbase":"04 ffff 001d 0104 4554 6865 2054 696d 6573 2030 332f 4a61 6e2f
Times headline      3230 3039 2043 6861 6e63 656c 6c6f 7220 6f6e 2062 7269 6e6b 206f
                    6620 7365 636f 6e64 2062 6169 6c6f 7574 2066 6f72 2062 616e 6b73"
    }
  ],
  "out":[
    {
    "value":"50.00000000",
    "scriptPubKey":"04 678a fdb0 fe55 4827 1967 f1a6 7130 b710 5cd6 a828 e039
                    09a6 7962 e0ea 1f61 deb6 49f6 bc3f 4cef 38c4 f355 04e5 1ec1
                    12de 5c38 4df7 ba0b 8d57 8a4c 702b 6bf1 1d5f OP_CHECKSIG"
    }
  ]
  }
],
"mrkl_tree":[
  "4a5e 1e4b aab8 9f3a 3251 8a88 c31b c87f 618f 7667 3e2c c77a b212 7b7a fded
   a33b"
]
}
```

The process of a transaction

As has already been explained, a transaction consists of various fields, amongst them the inputs and outputs. Figure 15 shows the dump of one of the transactions included in the block 278569 (dated 4 January, 2014).

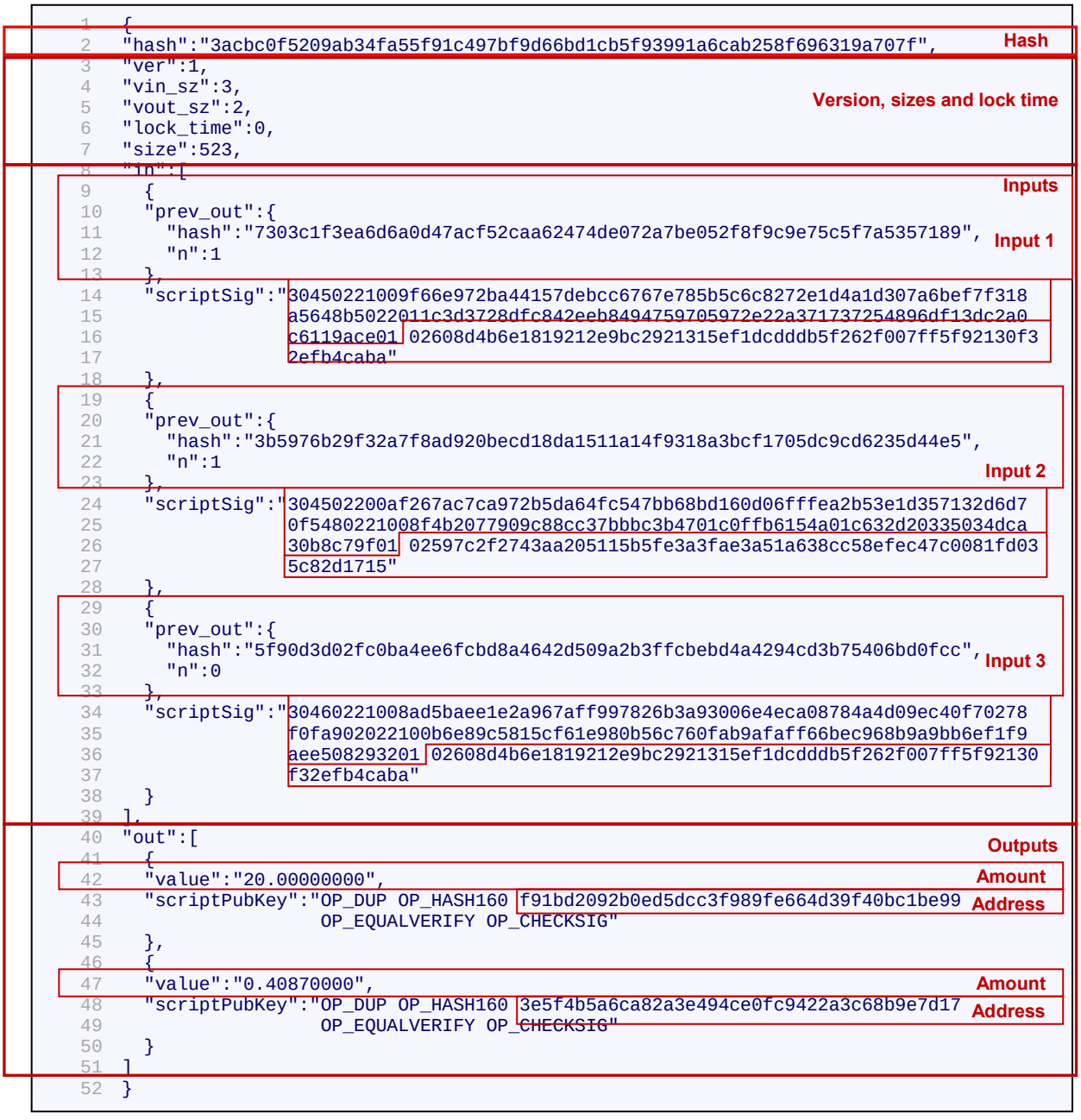
- In line 2 is the transaction's hash, i.e. the rest of the fields combined and encoded by the SHA-256 function.
- Lines 3 and 6 follow the format previously defined:
  - "`ver`": the current version number (1).
  - "`vin_sz`": the number of inputs in the transaction. In this case, 3.
  - "`vout_sz`": the number of outputs in the transaction. In this case, 2.

- "`lock_time`": until when will the transaction be blocked. Value 0 indicates the transaction is not blocked.

In addition, the header includes the size of the transaction in bytes, in this case 523.

- Between lines 8 and 39 the list of inputs appears:
  - The origin of each input is specified through the structure "`prev_out`". This structure includes:
    - The transaction hash produced as an output. For example, the transaction hash which produced the first input is `7303c1f3ea…` (line 11).
    - In addition, the "`n`" field specifies which output (counting from 0) of all the outputs produced the transaction. For example, the first input was the second output of the previous transaction, hence "`n: 1`" (line 12).
  - Each input also includes the **"`scriptSig`"** field, which contains two very important values, separated by a space:
    - The transaction's signature, for example **"`30450…ace01`"** (lines 14 to 16) of the first input.
    - The public key of the payer associated with the input address. For example, "`0260…caba`" (lines 16 and 17) of the first input.

Figure 15. Dump of the transaction.
3acbc0f5209ab34fa55f91c497bf9d66bd1cb5f93991a6cab258f696319a707f.




```
1  {
2  "hash":"3acbc0f5209ab34fa55f91c497bf9d66bd1cb5f93991a6cab258f696319a707f",
3  "ver":1,
4  "vin_sz":3,
5  "vout_sz":2,
6  "lock_time":0,
7  "size":523,
8  "in":[
9    {
10   "prev_out":{
11     "hash":"7303c1f3ea6d6a0d47acf52caa62474de072a7be052f8f9c9e75c5f7a5357189",
12     "n":1
13   },
14   "scriptSig":"30450221009f66e972ba44157debcc6767e785b5c6c8272e1d4a1d307a6bef7f318
15                a5648b5022011c3d3728dfc842eeb8494759705972e22a371737254896df13dc2a0
16                c6119ace01 02608d4b6e1819212e9bc2921315ef1dcdddb5f262f007ff5f92130f3
17                2efb4caba"
18   },
19   {
20   "prev_out":{
21     "hash":"3b5976b29f32a7f8ad920becd18da1511a14f9318a3bcf1705dc9cd6235d44e5",
22     "n":1
23   },
24   "scriptSig":"304502200af267ac7ca972b5da64fc547bb68bd160d06fffea2b53e1d357132d6d7
25                0f5480221008f4b2077909c88cc37bbbc3b4701c0ffb6154a01c632d20335034dca
26                30b8c79f01 02597c2f2743aa205115b5fe3a3fae3a51a638cc58efec47c0081fd03
27                5c82d1715"
28   },
29   {
30   "prev_out":{
31     "hash":"5f90d3d02fc0ba4ee6fcbd8a4642d509a2b3ffcbebd4a4294cd3b75406bd0fcc",
32     "n":0
33   },
34   "scriptSig":"30460221008ad5baee1e2a967aff997826b3a93006e4eca08784a4d09ec40f70278
35                f0fa902022100b6e89c5815cf61e980b56c760fab9afaff66bec968b9a9bb6ef1f9
36                aee508293201 02608d4b6e1819212e9bc2921315ef1dcdddb5f262f007ff5f92130
37                f32efb4caba"
38   }
39 ],
40 "out":[
41   {
42   "value":"20.00000000",
43   "scriptPubKey":"OP_DUP OP_HASH160 f91bd2092b0ed5dcc3f989fe664d39f40bc1be99
44                  OP_EQUALVERIFY OP_CHECKSIG"
45   },
46   {
47   "value":"0.40870000",
48   "scriptPubKey":"OP_DUP OP_HASH160 3e5f4b5a6ca82a3e494ce0fc9422a3c68b9e7d17
49                  OP_EQUALVERIFY OP_CHECKSIG"
50   }
51 ]
52 }
```

It should be noted that the amount of money involved in the transaction does not appear in any of the inputs. This is so because the total funds of each input address are transferred to the output addresses.

Finally, there are the outputs (lines 40 to 51), in this case two:

- In the "value" field, the amount of cash transferred to each output is specified. For example, in the case of the first a total of 20 bitcoins is transferred (line 42), while in that of the second the total is of 0.4807 bitcoins (line 47).
- In addition, each output has a "scriptPubKey" field (lines 43 and 44 for the first output, and lines 48 and 49 for the second) which includes various data in a single chain. The most important is the hash, which identifies the output address. For the first output, the address is "f91b…be99" (line 43). The remainder of the values are commands in Bitcoin's own scripting language. One of the addresses may be that of the payee client and the other that of the payer, used to receive change, although from a single payment it is difficult to say which is which. In this example it will be assumed that the first address is that of the payee, and the second for receipt of change.

Recalling the process of a Bitcoin transaction, in the case of the real data of the transaction that has just been analysed what occurs is the following:

1. The previous addresses related to this transaction are:
    1. The second output ("n: 1") of the transaction "7303…7189".
    2. The second output ("n: 1") of the transaction "3b59…44e5".
    3. The first output ("n: 0") of the transaction "5f90…0fcc".
2. The payer uses the private keys corresponding to the public keys "0260…caba", "0259…1715" and "0260…caba" to generate the digital signatures which show that funds are being transferred from each of the input addresses to the output addresses. The signatures produced are, respectively: "3045…ce01", "3045…9f01" and "3046…3201". Note that the first and third public keys coincide. This means that the payer uses the same pair of keys for both addresses.
3. In the outputs, the payer specifies that the address "f91b…be99" will receive 20 bitcoins and the address "3e5f…7d17" 0.4807 bitcoins. The payer then disseminates the transaction to the rest of the network. Eventually, it will reach a miner who will decide to include it in the next block. In this case, the transaction which has been analysed was included in the block 278569 (dated 4 January, 2014). How was this done, will be seen in the following section.

Mining a new block

As has already been mentioned, mining is a process of creating new blocks, being a computationally costly task.

Figure 16 shows the content of block 278569, which will be analysed in order to explain the mining process in detail.

The header of the block shown includes the following fields:

- "ver" (line 3): the block version, in this case, 2.
- "prev_block" (line 4): the hash of the previous block, with the value "0000000000000010...a1e5".
- "mrkl_root" (line 5) the current Merkle tree root hash, with the value "ea7f…7c8d"
- "time" (line 6): the Unix time of the block's creation, "1388837339".
- "bits" (line 7): the complexity of the current block, set at "419628831".

- “nonce” (line 8): the proof-of-work nonce, here “1183905159”.

Next, the information relating to the transactions included in the block:

- “n_tx” field (line 9): the number of transactions included in the block, here “267”.
- “size” field (line 10): the number of bytes which follows.
- “tx” field (lines 11 and 12): the list of transactions, similar to that seen in the previous section (omitted in Figure 16 for readability).

Finally, in lines 23 and 27 of the dump shown in Figure 16, is included the content of the Merkle tree (with several intermediate lines omitted), which allows the verification of the correct inclusion of the block in the blockchain.

Figure 16. Dump of the block 278569.

```
1  {
2    "hash":"00000000000000010d3c12aba4e30310a7ab44062a9acef2a2ef796ceaa0a313",
3    "ver":2,
4    "prev_block":"00000000000000010f506a248cb023addb43b06874f77e0e5fd78036af0ea1e5",
5    "mrkl_root":"ea7f525d9e7ab577063abf00142e183022396e4b54ce7a813769172a48337c8d",
6    "time":1388837339,
7    "bits":419628831,
8    "nonce":1183905159,
9    "n_tx":267,
10   "size":146355,
11   "tx":[
12     {
13       "hash":"573d733ad6f6b7203ebee4e266cee48df8ac1dc876185cdd1a5b4b188a1cb242",
14       "ver":1,
15       "vin_sz":1,
16       "vout_sz":434,
17       "lock_time":0,
18       "size":14879,
19       "in":[ … ],
20       "out":[ ... ]
21     }, …
22   ],
23   "mrkl_tree":[
24     "573d733ad6f6b7203ebee4e266cee48df8ac1dc876185cdd1a5b4b188a1cb242",
25     ...
26     "ea7f525d9e7ab577063abf00142e183022396e4b54ce7a813769172a48337c8d"
27   ]
28 }
```

Header

Transactions

Merkle tree

The most interesting part here concerning mining is the “bits” and “nonce” fields, and the first value of all, the ”hash” field. The block’s hash is calculated using the header fields[41], i.e. in this case the values “2”, “00000000000000010...a1e5”, “ea7f…7c8d”, “1388837339”, “419628831” y “1183905159”, corresponding to the “ver”, “prev_block”, “mrkl_root”, “time”, “bits” and “nonce” fields, respectively.

[41] https://en.bitcoin.it/wiki/Block_hashing_algorithm

The "bits" field is used to determine if a hash is valid. Specifically, this field is an encoded version of the maximum value which the block's hash can have to be so considered. To find the limit, the value of the "bit" field is first converted into hexadecimal. In this case, 419628831 in base 10 is converted into 0x1903071F in base 16. Then, the following formula is applied [42]:

$$0x03071F * 2 ** (8 * (0x19 - 3)) = 0x3071F000000000000000000000000000000000000000000000$$

Any hash with a value less than this hexadecimal number will be valid. Applying the SHA-256 function to the above header values (using adequate encoding) gives the value specified in the "hash" parameter "000000000000000010d3c12aba4e30310a7ab44062a9acef2a2ef796ceaa0a313", which is less than the limit value and is, therefore, a valid hash. Note that all the fields from which the hash is calculated, except the "nonce", are fixed. It is therefore the "nonce" field which determines the validity of the hash, and it is this that miners have to vary until a valid hash is found. Obviously, the lower the limit value, the more difficult it is to find a valid nonce (since the number of values which satisfy the formula is reduced).

Rewards

Given that calculating new blocks is very costly, the miner or miners who find new blocks receive a reward.

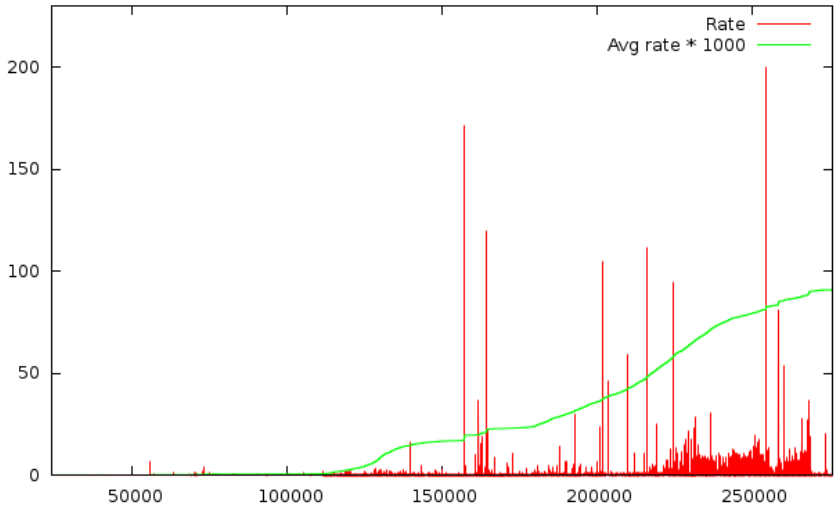
This reward can arrive in one of two ways. First, Bitcoin has established a maximum limit of 21 million bitcoins, and until that limit is reached, the generation of each new block is rewarded with a predefined amount of *new* bitcoins. For example, until November 2012, the reward for each new block was 50 bitcoins. Since then, the reward has been 25, and it is estimated that the reward will be halved again during 2016.

Second, so that the motivation for the miners stays the same despite the fall in their reward (which will eventually reach zero), there are transaction fees, through which users "donate" a part of the money involved in a transaction to the miner who verifies it. Figure 17 shows how the transaction fees have evolved since the start of Bitcoin is shown. The red line shows the transaction fee for each block, while the green line shows the average fee accumulated up to the number of the then current block (so as to be visible on the graph, it has been multiplied by a thousand). For instance, around block number 255,000, there was a block for which approximately 200 bitcoins were paid (which appears an extraordinarily exceptional case), while up to approximately block number 120,000 transaction fees were practically negligible. In terms of the average value of fees, it can be seen that it rises steadily. For example, around block 150,000 the transaction fee stood at more or less 0.02 bitcoins (20 / 1000), while around block 270,000 the average transaction fee was around 0.09 bitcoins. (Note: as a source for these data, Bitcoin's own blockchain was used, using the *blockparser*[43] tool to obtain the data for each block.

[42] https://en.bitcoin.it/wiki/Difficulty

[43] https://github.com/znort987/blockparser

Figure 17. Evolution of Bitcoin transaction fees.



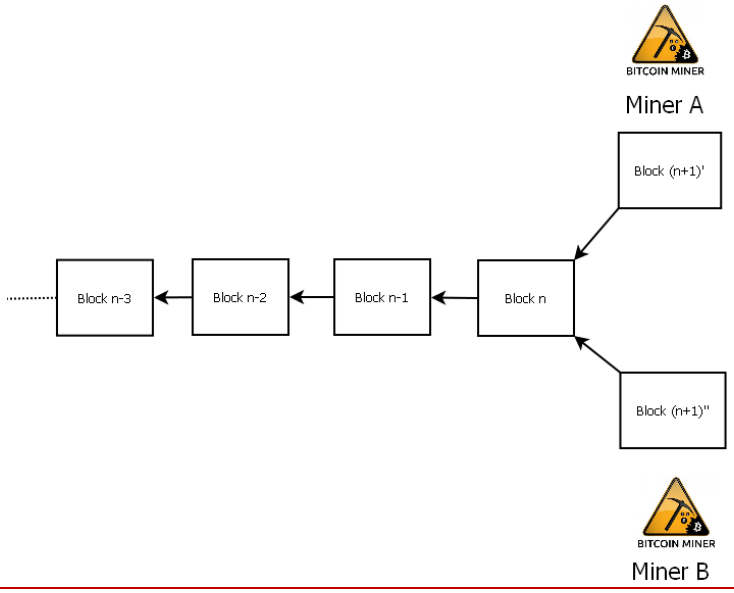
An additional feature, which helps protect Bitcoin against attackers or unanticipated scenarios, is that rewards (including new coins) earned through mining cannot be spent until 100 new blocks have been added to the chain. This feature is useful, for example, in avoiding cases in which those who generate a new block (thus creating new coins) and the miner who creates it use some of these bitcoins even though subsequently the block is rejected for not belonging to the larger chain. The term used for this concept is "*100-block maturation time*"[44].

Confirmation of a transaction

Even if a new transaction has been included in a block and that block in the chain, this can initially be reversed. This can happen if two initially valid branches are created, something that can occur for diverse reasons. For example, like it happened in the mentioned incident of March 2013 seen in section on Economic considerations. This can also happen if two miners verify new blocks at the same time. This scenario is shown in Figure 18.

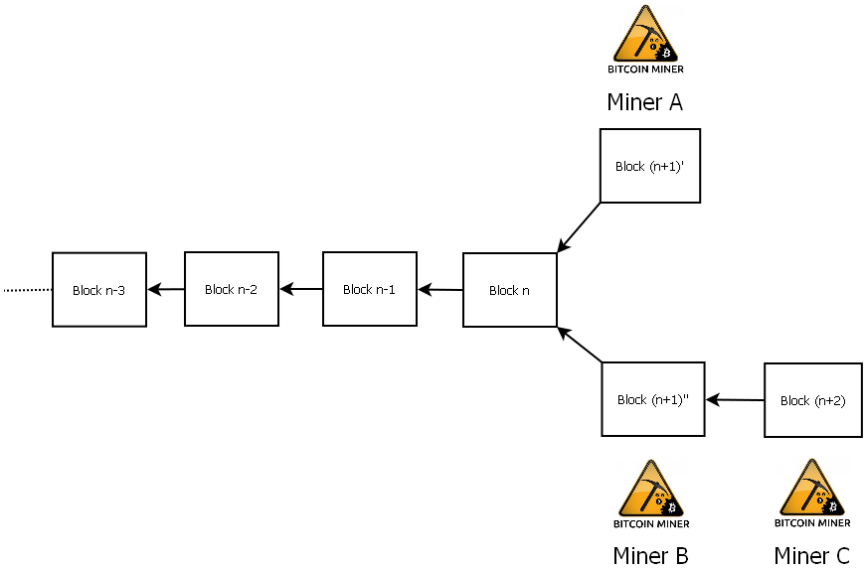
[44] https://en.bitcoin.it/wiki/Block_chain

Figure 18. The creation of two branches in the blockchain.



When two branches are generated, each will initially be backed up by a given number of miners, who will go on extending it. Additionally, the more alike the branches' computing power are, the longer it will take in resolving the anomaly, although eventually one of the branches will receive a block before the other, and will prevail, as shown in Figure 19.

Figure 19. The resolution of alternative branches.



This notwithstanding, given that taking as verified a block not supported by other blocks is not a good idea, it is advisable to wait for a given number of blocks before considering a transaction as confirmed. This number of blocks can vary depending on how many are involved in the transaction, and, obviously, on contingencies. Normally, after six new blocks the transaction will be difficult to reverse and can therefore be considered confirmed. Note

that the probability of reversing a transaction decreases exponentially with each new block that backs it up.

4 ANONYMITY AND PRIVACY IN BITCOIN

In general, Bitcoin is understood to be a system which guarantees the anonymity and privacy of its users [45]. Nevertheless, the privacy section[46] of the Bitcoin Wiki[47] observes that:

> *Bitcoin is often perceived as an anonymous payment network. But in reality, Bitcoin is probably the most transparent payment network in the world. [..] Since users usually have to reveal their identity in order to receive services or goods, Bitcoin addresses cannot remain fully anonymous.*

In other words, Bitcoin is a system of great transparency, fundamentally because anyone can consult the global history of transactions. It should be noted that although there exists the possibility of pruning transactions to save storage space there are always (publically accessible) nodes, called archive nodes, which hold the complete history. The reason behind this is to be able to verify with complete certainty that there have not been irregularities.

Even if it is true that there is no internal link between Bitcoin addresses and real identities, a user who wishes to make a payment in bitcoins will eventually have to provide some kind of indentifying data to whoever provides him with the service in question, such that his identity will be linked in some way with the address used to make the payment[48]. In such a case, it may be that the address of the payer can be used to identify other related addresses. This is why there are those who argue that it is impossible for a Bitcoin address to remain perfectly anonymous. As we saw in the Controversy section with regard to the case of Silk Road, these types of investigations have taken place in real operations.

Maybe part of the general confusion surrounding the anonymity provided by Bitcoin results from a statement made in the original “Satoshi Nakamoto” paper [1]:

> *[..] privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.*

From the cryptographic point of view, however, this does not mean *literally* that the identity of the owner of these keys will remain anonymous. Rather, it means that the keys do not contain inside themselves a “real” identity. Despite this, as has already been observed, and as will be seen below, this does not mean that it would be impossible (or even in certain cases improbable) to deduce the real identity of someone who manages a Bitcoin address.

In any case, it deserves emphasising that Bitcoin as such, as a system, does not require that a user enters indentifying data and that, unlike traditional trading systems, there is no central authority to whom one could ask for the real identity of the owner of an account.

---

[45] See, for instance: http://www.wired.co.uk/news/archive/2013-05/7/bitcoin-101 ó http://shop.wikileaks.org/donate#dbitcoin

[46] http://bitcoin.org/en/protect-your-privacy

[47] http://bitcoin.org/en/protect-your-privacy

[48] It is customary and a good practice in privacy studies to consider that privacy is lost in the momento in which any information considered prívate is revealed to any entity other than that which privacy is under analysis.

Tracing Bitcoin users

Below we will summarise the main methods to de-anonymise Bitcoin.

Tracing based on analysis of traffic

As the authors of "*An Analysis of Anonymity in the Bitcoin System*" [5], point out, citing Dan Kaminsky, it is possible to discover the identity of someone who makes a payment in Bitcoin through an analysis of TCP/IP traffic. Owing to Bitcoin's design, the first person to publicise a transfer will probably be the payer. Therefore, discovering who the first person to publicise it was will permit in all probability to know who is the payer in the transaction and who the owner of the input addresses used are.

On how to do this, Dan Kaminsky notes that the costs to establish a connection to all the nodes active at a given instant of time[49] are assumable. This can vary with time, according to the volume of the Bitcoin network. Since Kaminsky made these observations, the network has grown considerably: according to the *getaddr* Bitnodes service[50], on 14 January 2014 there were approximately 127,741 nodes connected. In any case, although it might not be possible to establish a connection to all the nodes, it will always be possible to make directed attacks, analysing segments of the network probably related to specific objectives.

It should also be noted that such an attack would be based on Bitcoin's own structure (specifically, that the first person to publicise a transaction will be the payer). For this reason, Bitcoin on its own would find it difficult to prevent such an attack. To deal with this, however, it should only be necessary to use a system of communication anonymisation, such as Tor.

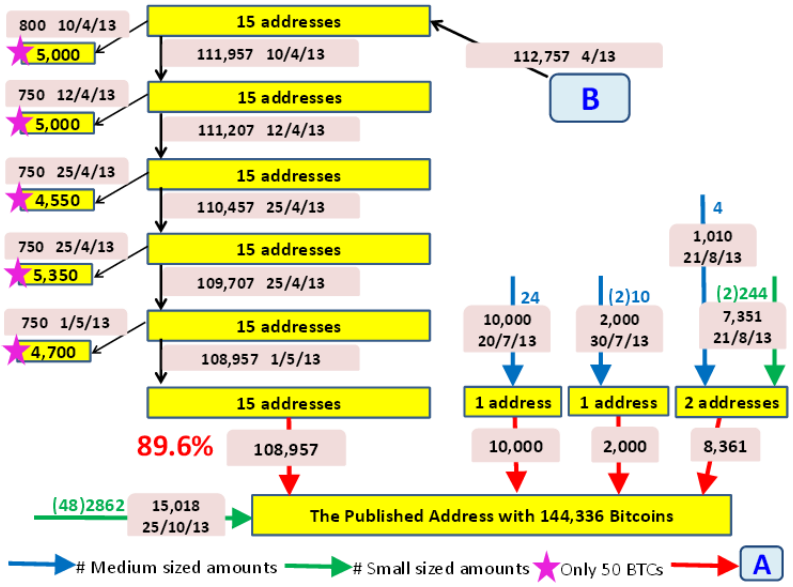
Tracing based on heuristics

Another type of analysis which stands out is that based on the relations which may be established between addresses that, in a given moment, appear as common inputs in a transaction. Given the construction of Bitcoin, the fact that an entity uses various Bitcoin addresses as an input in the same transaction guarantees that that entity controls the private keys associated with these addresses. Therefore, it seems safe to assume that all these addresses belong to the same person. Applying this and similar principles, various studies have developed heuristics to reduce the degree of anonymity of Bitcoin users [6] [7]. For example, the authors of "*Evaluating User Privacy in Bitcoin*" [6] estimate that approximately 40% of Bitcoin users could be identified using the heuristics set out in the study.

A striking result, obtained applying this type of measure, is that published at the end of 2013 by Ron and Shamir [7], in which a relation between the founder of Silk Road and someone who was probably one of the creators of Bitcoin was established. Figure 20 shows a part of this analysis. Short after the publication of this work, the owner of the bitcoins to which the tracing seem to point at refuted this connection. Nevertheless, the tracing capability shown by the researchers remains completely valid.

[49] http://dankaminsky.com/2011/08/05/bo2k11/
[50] http://getaddr.bitnodes.io/chart/nodes/

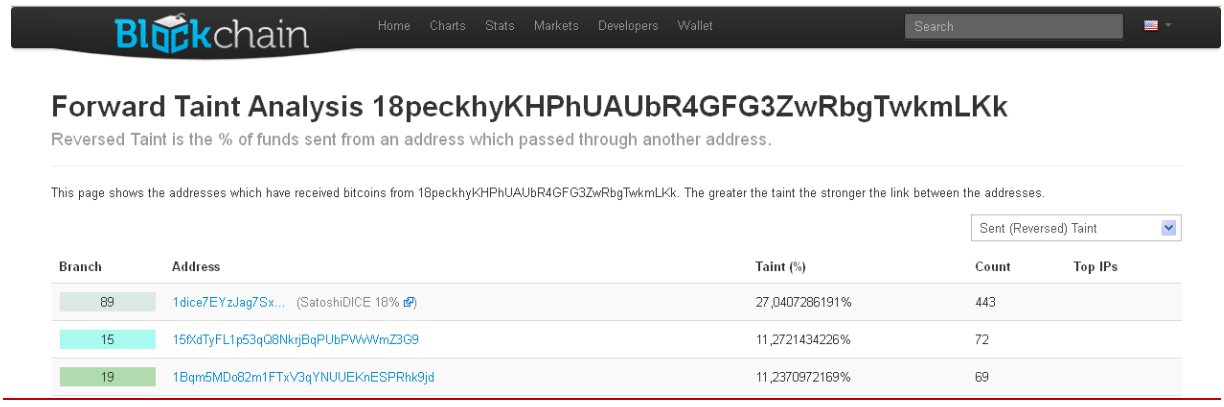
Figure 20. Trace of the founder of Silk Road's money.



Source: "How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth", [7]

Another illustrative example of this type of analysis can be directly accessed from the Blockchain website https://blockchain.info/taint/ where, appending an address's hash to the URL, a list of related addresses, including the *taint* value, is displayed, as shown in Figure 21. This value indicates the correlation between the address consulted and others, even including the identity of that which it is associated with (see, for example, the first transaction in the figure, in which it is indicated (with 18% of probability) that the first address belongs to "*Satoshi Dice*", a bitcoin gambling site.

Figure 21. An example of a blockchain taint analysis.



Nevertheless, in the same way that tracing users through the analysis of TCP/IP traffic can be mitigated, it is also possible to reduce the effectiveness of these attacks on privacy too. To do this, it would be necessary to keep a partition of the Bitcoin addresses controlled by a single person, assuring that addresses from two distinct subsets are never used as inputs in the same transaction.

Mixing services

An advanced measure to enhance Bitcoin users' anonymity, and hence privacy, is provided by what are known as mixing services [9], named after the homonym services proposed in 1981 by David Chaum to anonymise communications [10]. These services employ a set of Bitcoin addresses to which users can transfer bitcoins. After a given delay – to prevent timing attack analyses – the user will have their bitcoins returned from another address, not related with his own. In [9], three of these services are analysed, using pre-established metrics to estimate their level of anonymity. The study concludes that two of these services (Bitcoin Fog[51] and Blockchain Send Shared[52]) provide a high degree of anonymity, while the third (BitLaundry[53]) does not.

However, using these services requires a high degree of trust on the part of users (which runs against Bitcoin's philosophy of not requiring the use of trustworthy authorities). This is the case for two reasons. First, one has to trust the services not to keep a log of transactions that could be leaked; and second, there have been cases of dishonest services that have not returned deposited bitcoins, as the authors of [7] note in the case of the (now apparently inactive) BitMix service.

[51] http://www.bitcoinfog.com/
[52] https://blockchain.info/es/wallet/send-shared
[53] http://app.bitlaundry.com/

5 CONCLUSIONS: STRENGTHS AND WEAKNESSES

To conclude this technical analysis of the architecture and functioning of this system of electronic cash, here the main strengths and weaknesses of the Bitcoin system are summarised.

STRENGTHS

Distributed trust

In traditional models, trust is deposited in an authority or entity which controls all the relevant information. In Bitcoin, conversely, there is no such authority; rather, information is managed by the users as a whole. In this way, whenever more than half of the users of the system are honest, the "rules" set out by the system cannot be broken by any dishonest users.

Incentives

By convention, until the limit of 21 million bitcoins is reached, when a miner builds a new block they are rewarded with a predefined amount of bitcoins. In this way all the nodes have an incentive to support the network, and a way of creating and distributing cash is defined, which is necessary given that there is no central authority minting new money,.

These incentives can also be provided through fees for the verification of transactions, such that the user who creates a valid block receives as a payment a part of the money involved in the verified transaction.

Cryptography

The use of a strong asymmetric cryptographic system, like ECDSA, and of robust hash algorithms, like SHA-256, guarantees the current integrity of the system. But taking into account that computing capacity increases year on year, in addition to the appearance of new advances in cryptographic and cryptanalytic theory, it is not unreasonable to believe that algorithms that are secure today will not be tomorrow. It is for this reason that the system is designed in such a way that the cryptographic system used can be changed, using the same peer-to-peer protocol and transaction management. It is simply a question of allowing, should it be necessary, new transactions to use a different cryptographic system[54].

Scalability

As has already been seen, Bitcoin works with peer-to-peer communications, for which its growth is based on the adhesion of new nodes to the network.

However, it must not be forgotten that Bitcoin's functioning is based on cryptography, and specifically on the use of ECDSA (leaving aside the RIPEMD-160 and y SHA-256 operations, which are sufficiently rapid not to have to take them into account with regard to scalability). Calculations carried out on the implementation of ECDSA indicate that some 8,000 verifications of digital signatures a second can be carried out by a current desktop processor. The most recent data from Bitcoin Watch show that around 2,500 transactions an hour –

[54]This design philosophy that "ignores" the cryptographic primitives that may be applied is known as "Dolev-Yao". This model assumes that the cryptographic building blocks are perfect, allowing the design of a system focusing just in the communication protocols.

about 0.7 per second – are performed. The network would have to experience spectacular growth indeed to reach the theoretical limits of its functioning.

When it comes to scalability, storage necessities also need to be taken into account. Bitcoin keeps a list of all the transactions that have been realised in the network since its beginning. This suggests that the blockchain will grow in time without limit. Nevertheless, it should be remembered that most transactions can be eliminated from the blockchain, allowing the size of this to fall notably.

According to the original paper describing Bitcoin [1], where it was anticipated that the block header would be 80 bytes, and taking into account the creation of blocks every ten minutes, the chain will grow 4.2MB a year (80 bytes * 60 minutes/10 minutes * 24 hours * 365 days).

Transparency

As its own wiki observes, Bitcoin is probably the most transparent electronic payment system that has ever existed. This is due to the fact that anyone is able to consult the complete transaction history, and know where each amount of money has come from and where each has gone. This, for example, permits the "marking" of stolen money, or money which has been used in illegitimate activities, in such a way that any potential payee can subsequently reject it. Nevertheless, this is not always seen as positive[55].

WEAKNESSES

Vulnerabilities

Throughout the Bitcoin network's life, vulnerabilities have been discovered in the different implementations that have appeared, which can be exploited by malicious users for different ends, from the theft of bitcoins or double-spending, to causing the whole network to malfunction. A table of the five most serious vulnerabilities is shown in Appendix II; and a full list of vulnerabilities can be found in the *Open Sourced Vulnerability Database*[56].

Theft from wallets

The design of the Bitcoin wallet as such does not entail its encryption, since this is a security measure left to the discretion of the user. By default, most wallets are stored unencrypted, which makes the appearance of malware specifically designed to rob wallets possible. However, there are exist wallets which include the option of encryption.

In this respect, special care needs to be taken with regard to back-up copies of wallets: owing to how the system functions, bitcoins stored in a more recent wallet version could be accessed through a back-up copy with an old password.

Unencrypted traffic

Communication between peers is unencrypted. Although this does not impact on Bitcoin strongly (any user can connect to the network and access the totality of transactions), it is something to be borne in mind, since according to the needs of the user, complementary security measures should be implemented.

[55] http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/
[56] http://osvdb.org/search?search[vuln_title]=bitcoin

According to how Bitcoin functions, a malicious user can spy on another user's traffic and identify the transactions they carry out by simply comparing incoming and outgoing transactions.

Energy Consumption

The value of a bitcoin is inextricably related to the consumption of energy. Mining is carried out through computing operations, and to do this equipment has to be functioning and connected to an energy source, with the consumption of energy that this supposes.

Taking into account the increasing difficulty that the network introduces for the mining of bitcoins and the cost of electricity, in the long-term mining will cease to be profitable. For this reason, transaction fees will have to increase to keep the system sustainable. This lowering of profitability, however, may also make users abandon the network for others with lower costs.

Anonymity and privacy

Although Bitcoin as such does not require the user to enter indentifying data to use it, the level of anonymity the system provides can be significantly reduced through independent means based on the construction and functioning of the system itself; means, therefore, at times difficult to prevent. Although a thorough management of Bitcoin addresses can mitigate this problem, doing this effectively can turn out to be difficult.

Taking this into account, given that the amount of cash in bitcoins in any address is publically available information, not only can the money owned by a person whose identity has been compromised be deduced, but where that money has come from and where it has gone can also be known too. Without any doubt, this supposes a serious danger for people's privacy (and even integrity) should Bitcoin ever be taken up on a massive scale.

REFERENCES

CITED ARTICLES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] D. Ron and A. Shamir, "How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?," 2013. [Online]. Available: http://eprint.iacr.org.

[3] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," vol. 28, no. 10, 1985.

[4] Certicom Research, "SEC 2: Recommended Elliptic Curve Domain Parameters," 2010.

[5] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," 2011.

[6] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating User Privacy in Bitcoin," vol. Financial Cryptography and Data Security, 2013.

[7] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," 2013.

[8] M. Möser, "Anonymity of Bitcoin Transactions," Münster Bitcoin Conference, 2013.

[9] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84-88, 1981.

OTHER REFERENCES

- *Aviso a los consumidores sobre las monedas virtuales*, accessed 27/01/2014, http://www.eba.europa.eu/documents/10180/16136/EBA_2013_01030000_ES_TRA1_Vinay.pdf.
- *The Mail Archive post: Bitcoin P2P e-cash* paper, accessed 27/01/2014, https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html.
- *Bitcoin open source implementation of P2P currency*, accessed 27/01/2014, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.
- *Portal de Bitcoin*, accessed 01/24/2014, http://www.bitcoin.org.
- *Possible Economic Consequences of Digital Cash*, accessed 01/24/2014, http://www.isoc.org/inet96/proceedings/b1/b1_1.htm.
- *Bitcoin is evil*, accessed 27/01/2014, http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/.
- *La banca china no operará con bitcoins*, accessed 01/24/2014, http://tecnologia.elpais.com/tecnologia/2013/12/05/actualidad/1386240024_458907.html.
- *eBay to allow Bitcoin sales in 'virtual currency' category,* accessed 01/24/2014, http://news.cnet.com/8301-1023_3-57617502-93/ebay-to-allow-bitcoin-sales-in-virtual-currency-category/.
- *Google Lets Slip That It's Exploring Possible Bitcoin Integration Plans*, accessed 01/24/2014, http://www.forbes.com/sites/andygreenberg/2014/01/22/google-lets-slip-that-its-exploring-possible-bitcoin-integration-plans/.
- *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, accessed 01/24/2014, http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.
- *Bitcoin Trade*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Trade.
- *Red Tor: anonimato y vulnerabilidades*, accessed 01/24/2014, http://inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/red_tor_anonimato_vulnerabilidades.
- *Silk Road: Not Your Father's Amazon.com*, accessed 01/24/2014, http://www.npr.org/2011/06/12/137138008/silk-road-not-your-fathers-amazon-com.
- *End Of The Silk Road: FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market*, accessed 01/24/2014, http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/.

- *Why do bitcoins have value?*, accessed 01/24/2014, http://bitcoin.org/en/faq#why-do-bitcoins-have-value.
- *Bitcoin Network Shaken by Blockchain Fork*, accessed 01/24/2014, http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/.
- *Linode Hacks*, accessed 01/24/2014, https://bitcointalk.org/index.php?topic=83794.0#post_linode_hacks.
- *Silk Road Seizure*, accessed 01/24/2014, https://bitcointalk.org/index.php?topic=83794.0#post_silk_road_seizure.
- *Yahoo malware enslaves PCs to Bitcoin mining*, accessed 01/24/2014, http://www.bbc.co.uk/news/technology-25653664.
- *Bitcoin development*, accessed 01/24/2014, http://bitcoin.org/en/development.
- *Bitcoin Clients*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Clients.
- Notable cryptocurrencies, accessed 01/24/2014, http://en.wikipedia.org/wiki/List_of_cryptocurrencies.
- *Mining digital gold*, accessed 01/24/2014, http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital.
- *ECDSA*, accessed 01/24/2014, http://es.wikipedia.org/wiki/ECDSA.
- *DER* Encoding, accessed 01/24/2014, http://en.wikipedia.org/wiki/Distinguished_Encoding_Rules.
- *SHA*, accessed 01/24/2014, http://es.wikipedia.org/wiki/Secure_Hash_Algorithm.
- *RIPEMD-160*, accessed 01/24/2014, http://es.wikipedia.org/wiki/RIPEMD-160.
- *Android Security Vulnerability: 11 August 2013*, accessed 01/24/2014, http://bitcoin.org/en/alert/2013-08-11-android.
- *Elliptic Curve DSA, Signature generation algorithm*, accessed 01/24/2014, http://en.wikipedia.org/wiki/Elliptic_Curve_DSA#Signature_generation_algorithm.
- *Hashcash*, accessed 01/24/2014, http://en.wikipedia.org/wiki/Hashcash.
- *Bitcoin Network*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Network.
- *Satoshi Client Node Discovery*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery.
- *Bitcoin Protocol Specification: Message Types*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Protocol_Specification#Message_types.
- *Bitcoin: Codificación Base58Check*, accessed 01/24/2014, https://es.bitcoin.it/wiki/Codificaci%C3%B3n_Base58Check.
- *Bitcoin Transactions*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Transactions.
- Bitcoin blocks, accessed 01/24/2014, https://en.bitcoin.it/wiki/Blocks.
- *Block Hashing Algorithm*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Block_hashing_algorithm.
- *Blockchain: Gastos Duplicados*, accessed 01/24/2014, https://blockchain.info/double-spends.
- *Bitcoin Difficulty*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Difficulty.
- *Blockparser*, accessed 01/24/2014, https://github.com/znort987/blockparser.
- *Blockchain*, accessed 01/24/2014, https://en.bitcoin.it/wiki/Block_chain.
- *A simple guide to Bitcoin*, accessed 01/24/2014, http://www.wired.co.uk/news/archive/2013-05/7/bitcoin-101.
- *Wikileaks dontations*, accessed 01/24/2014, http://shop.wikileaks.org/donate#dbitcoin.
- *Bitcoin: Protect your Privacy*, accessed 01/24/2014, http://bitcoin.org/en/protect-your-privacy.
- *Black Ops Of TCP/IP 2011*, accessed 01/24/2014, http://dankaminsky.com/2011/08/05/bo2k11/.
- *Bitnodes*, accessed 01/24/2014, http://getaddr.bitnodes.io/chart/nodes/.
- *I Am Not Satoshi,* accessed 04/01/2014, http://blog.dustintrammell.com/2013/11/26/i-am-not-satoshi/
- *Partición de un conjunto*, accessed 01/24/2014, http://es.wikipedia.org/wiki/Partici%C3%B3n_%28matem%C3%A1tica%29.
- *Bitcoin Fog*, accessed 01/24/2014, http://www.bitcoinfog.com/.
- *Blockchain Send Shared*, accessed 01/24/2014, https://blockchain.info/es/wallet/send-shared.
- *BitLaundry*, accessed 01/24/2014, http://app.bitlaundry.com/.
- *Anti-Theft Bitcoin Tracking Proposals Divide Bitcoin Community*, accessed 01/24/2014, http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/.
- *OSVDB*, accessed 01/24/2014, http://osvdb.org/search?search[vuln_title]=bitcoin.

LIST OF FIGURES AND TABLES

FIGURES

Figure 1. “Satoshi Nakamoto’s” post to the cryptography mailing list. 6
Figure 2. “Satoshi Nakamoto’s” message on the P2Pfoundation. 7
Figure 3. California orders Bitcoin to cease operations. 9
Figure 4. Map of Businesses which accept bitcoins in Spain. 10
Figure 5. News report on the use of bitcoins in bars in Spain. 11
Figure 6. The depreciation of Bitcoin during the fork of March 2013. 12
Figure 7. Effect of the “Linode hacks” (02/03/2012) and the closing down of Silk Road (02/10/2013) on the price of bitcoins. 13
Figure 8. The effects of People’s Bank of China to bar the handling of Bitcoin transactions. 14
Figure 9. Cryptlocker ransom message. 15
Figure 10. The generic functioning of Bitcoin. 17
Figure 11. A transaction. 22
Figure 12. Transaction signatures. 22
Figure 13. Blocks and transaction pruning. 24
Figure 14. The genesis block. 26
Figure 15. Dump of the transaction 3acbc0f5209ab34fa55f91c497bf9d66bd1cb5f93991a6cab258f696319a707f. 28
Figure 16. Dump of the block 278569. 30
Figure 17. Evolution of Bitcoin transaction fees. 32
Figure 18. The creation of two branches in the blockchain. 33
Figure 19. The resolution of alternative branches. 33
Figure 20. Trace of the founder of Silk Road’s money. 37
Figure 21. An example of a blockchain taint analysis. 37
Figure 22. An example of a Merkle tree. 45

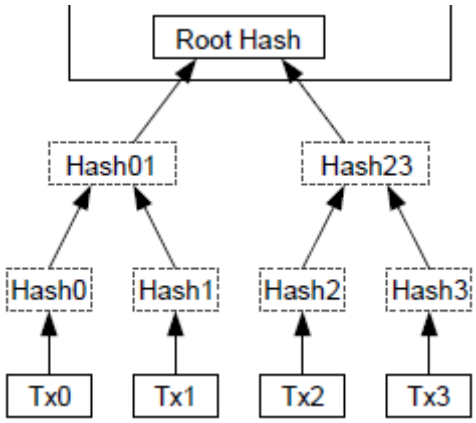
TABLES

Table 1. Transaction fields. 22
Table 2. Block fields. 23
Table 3. Block header 24

APPENDIX I – MERKLE TREES

Merkle trees of binary hashes. A binary tree is a data structure, in tree shape, where each node may have at most two child (hence, binary). Figure 22 illustrates how it works:

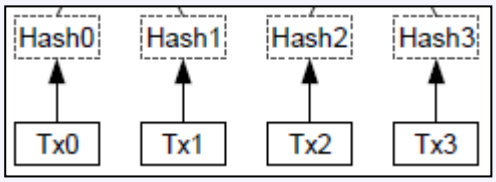
Figure 22. An example of a Merkle tree.



Source: "Bitcoin: A Peer-to-Peer Electronic Cash System", «Satoshi Nakamoto»

In the case of this example, the nodes are determined in the following manner:

1. The leaves of the tree: these are the nodes of the lower level. Each transaction which will form part of the block is double-hashed (SHA-256 of SHA-256 of the transaction).

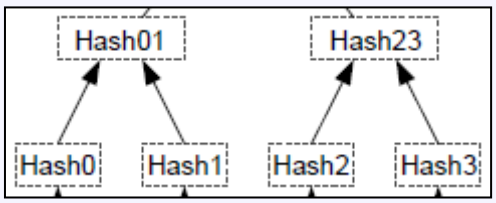



```
Hash0 = SHA256(SHA256(Tx0))
Hash1 = SHA256(SHA256(Tx1))
Hash2 = SHA256(SHA256(Tx2))
Hash3 = SHA256(SHA256(Tx3))
```

   a. If there is an odd number of transactions, the last double hash is duplicated, guaranteeing that the nodes are even.

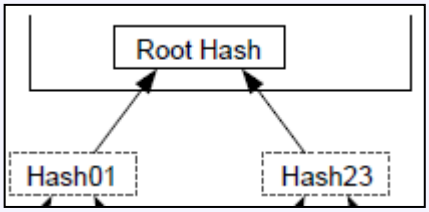
```
Hash3 = Hash2
```

2. Intermediate nodes: the hashes calculated from the lower level are grouped together in pairs and then double-hashed again. This is repeated recursively, such that each level has half the number of nodes than the next lower level.




```
Hash01 = SHA256(SHA256(Hash0+Hash1))
Hash23 = SHA256(SHA256(Hash2+Hash3))
```

3. The root: the single element at the top of the tree, called the **Merkle root**, and calculated in the same way as before.




```
Root Hash = SHA256(SHA256(Hash01+Hash23))
```

APPENDIX II – SUMMARY OF VULNERABILITIES

CVE-ID	Impact	Date	Title	Description
2012-4684	High	01/03/2013	bitcoind / Bitcoin-Qt Alert Signature Handling Remote DoS	bitcoind and Bitcoin-Qt contain a flaw that may allow a remote denial of service. The issue is triggered during the handling of a specially crafted signature alert. This may allow a remote attacker to cause a consumption of CPU or RAM resources, which will crash the system.
2013-2292	High	30/01/2013	bitcoind / Bitcoin-Qt Signature Verification Crafted Transaction Handling Remote DoS	bitcoind and Bitcoin-Qt contain a flaw that may allow a remote denial of service. The issue is triggered during signature verification when handling a specially crafted transaction that contains a saturation of content that uses SHA-256 hashing. This may allow a remote attacker to cause a consumption of CPU resources and a crash for the system.
2012-1910	High	16/03/2012	Bitcoin-Qt for Windows Malformed Bitcoin Protocol Message Handling Remote Code Execution	Bitcoin-Qt 0.5.0.x before 0.5.0.5; 0.5.1.x, 0.5.2.x, and 0.5.3.x before 0.5.3.1; and 0.6.x before 0.6.0rc4 on Windows does not use MinGW multithread-safe exception handling, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted Bitcoin protocol messages.
2010-5141	High	29/09/2010	wxBitcoin / bitcoind Bitcoin Transaction Unspecified Script Opcode Parsing Remote Bitcoin Theft	wxBitcoin and bitcoind contain a flaw that is triggered when the Bitcoin transaction code does not properly handle script opcodes. This may allow a remote attacker to spend other users' bitcoins.
2010-5139	High	29/07/2010	wxBitcoin / bitcoind Bitcoin Transaction Parsing Remote Overflow Bitcoin Creation	wxBitcoin and bitcoind are prone to an overflow condition. The program fails to properly sanitize user-supplied input resulting in an integer overflow. With a specially crafted transaction, a remote attacker can potentially create an excessive amount of bitcoins.