BITCOIN: A SOLUTION FOR PAYMENT SYSTEMS OR A SOLUTION IN SEARCH OF A PROBLEM?

2019

Carlos Conesa

Documentos Ocasionales
N.º 1901

BANCO DE ESPAÑA
Eurosistema

BITCOIN: A SOLUTION FOR PAYMENT SYSTEMS OR A SOLUTION IN SEARCH OF A PROBLEM?

BITCOIN: A SOLUTION FOR PAYMENT SYSTEMS OR A SOLUTION IN SEARCH OF A PROBLEM?

Carlos Conesa [*]

BANCO DE ESPAÑA

[*] The author wishes to thank Juan Ayuso, José Manuel Marqués, Sergio Gorjón and José Luis Romero for their comments.

Documentos Ocasionales. N.º 1901

2019

The Occasional Paper Series seeks to disseminate work conducted at the Banco de España, in the performance of its functions, that may be of general interest.

The opinions and analyses in the Occasional Paper Series are the responsibility of the authors and, therefore, do not necessarily coincide with those of the Banco de España or the Eurosystem.

The Banco de España disseminates its main reports and most of its publications via the Internet on its website at: http://www.bde.es.

ISSN: 1696-2230 (on-line edition)

Abstract

In October 2008 a mysterious article was published under the pseudonym Satoshi Nakamoto: “Bitcoin: a peer-to-peer electronic cash system”. Bitcoin’s entry into operation some months later in early 2009 barely caused a ripple. Since then, the scheme has accumulated more than half a million blocks in its blockchain and they include more than 300 million transactions. In view of the media impact of Bitcoin, it is worth explaining in some detail how Bitcoin works and what its limitations are. This article reviews the aims and basic functioning of Bitcoin, analyses its strengths and weaknesses, and discusses its usefulness as an exchange mechanism.

Keywords: blockchain, hash function, bitcoin, cryptoassets, cryptography, innovation, technology.

JEL classification: O31, O33.

Resumen

En octubre de 2008 se publicó un misterioso artículo bajo el seudónimo de Satoshi Nakamoto: «Bitcoin: a peer-to-peer electronic cash system». Meses después, a principios de 2009, Bitcoin comenzó a operar sin generar apenas atención. Desde entonces hasta hoy, el esquema ha acumulado más de medio millón de eslabones en su cadena de bloques o *blockchain,* que recogen más de 300 millones de operaciones. Teniendo en cuenta la repercusión mediática que ha generado *Bitcoin,* parece conveniente explicar con un cierto grado de detalle su funcionamiento y limitaciones. Este documento revisa los objetivos que se perseguían con la creación de Bitcoin y su funcionamiento básico, analiza sus ventajas e inconvenientes, y discute su utilidad como mecanismo de intercambio.

Palabras clave: *blockchain,* función *hash, bitcoin,* criptoactivos, criptografía, innovación, tecnología.

Códigos JEL: O31, O33.

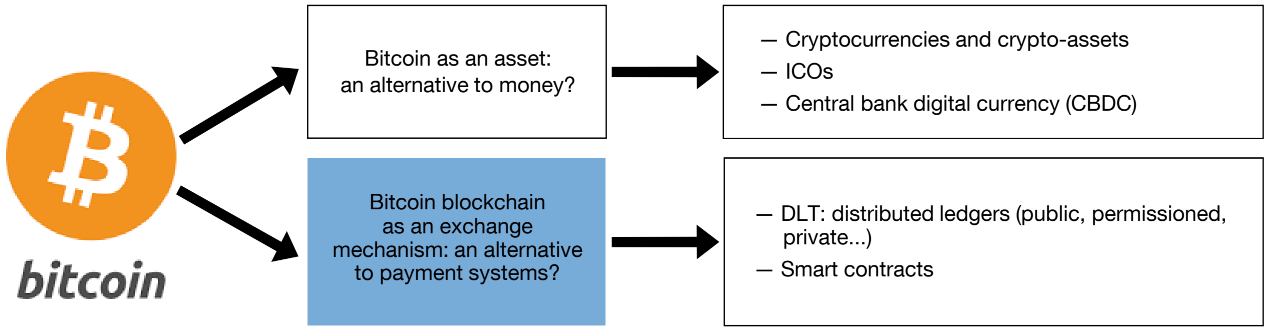
CONTENTS

1 Introduction

Bitcoin has attracted increasing interest in recent years and, moreover, the debate sparked by Bitcoin has ramified. Initially it branched into two areas of discussion. One was the role of bitcoins as an asset and the possibility that they might be an alternative to fiduciary money. The second was the analysis of the blockchain as an exchange mechanism and its potential use as a payment system or for the clearing and settlement of securities or other assets. Meanwhile, the market price of bitcoins has fluctuated sharply, from zero to nearly $20,000 per bitcoin. Currently (December 2018) its price is around $3,500 per bitcoin. As shown in Figure 1, the Bitcoin debate has become even more complicated. This paper focuses on the analysis of Bitcoin as an exchange mechanism, specifically on its strengths and weaknesses as an alternative to traditional payment systems.

COURSE OF THE DEBATE: FROM BITCOIN TO CRYPTO-ASSETS AND DISTRIBUTED LEDGER TECHNOLOGY (DLT)

FIGURE 1



Bitcoin as an asset: an alternative to money?

— Cryptocurrencies and crypto-assets
— ICOs
— Central bank digital currency (CBDC)

Bitcoin blockchain as an exchange mechanism: an alternative to payment systems?

— DLT: distributed ledgers (public, permissioned, private...)
— Smart contracts

SOURCE: Devised by author.

2 Why does Bitcoin function as it does?

This paper describes the functioning of the bitcoin exchange mechanism in somewhat more detail than is usually given in similar summaries. Although it avoids excessive technical details, some basic cryptographic concepts (hash functions and asymmetric cryptography) should be mastered. These basic concepts are explained in Box 1. Also, Bitcoin is presented differently from usual. Instead of diving straight into a description of how the scheme works, we take an iterative approach in which we build from scratch a cryptocurrency model similar to Bitcoin.[1] This procedure is slower, but the resolution of problems as they appear will be useful for explaining why Bitcoin functions as it does and not in some other way.

[1] Sections 2.1 and 2.2, which explain the iterative approach and the successive modifications to the proof-of-work protocol, are taken from Nielsen (2013), with some changes. The main change is that Bitcoin addresses are likened to account numbers rather than to currency references or serial numbers, which could cast doubt on their fungibility.

BASIC CONCEPTS: ASYMMETRIC CRYPTOGRAPHY AND HASH FUNCTIONS — BOX 1

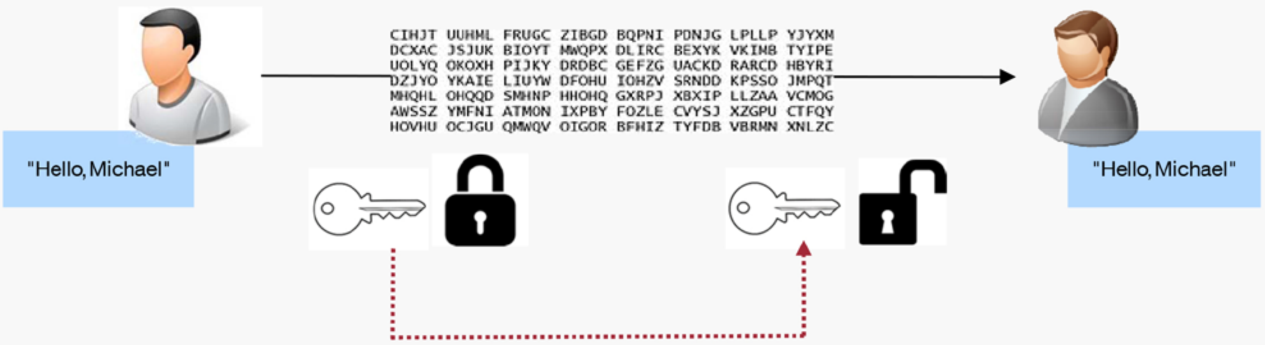
This box explains some basic concepts of cryptography relating to the functioning of Bitcoin described in the paper. The explanations are intended to make Bitcoin more generally understood: they are not intended to be rigorous, but rather to give a basic knowledge of how Bitcoin works.

Cryptography or encryption can be defined as a procedure which uses an algorithm with a key (cryptographic key) and transforms a message such that it is incomprehensible for anyone who does not have the secret key (decryption key) of the algorithm.

In its classical form, cryptography uses the same key to encrypt and decrypt messages, which does not fully solve the security problem. The recipients of the message have to exchange bilaterally the cryptographic key, and so run the risk that a third party may intercept that key and gain access to the information they are exchanging. Moreover, the number of bilateral key exchanges becomes unmanageable if the number of participants exchanging information is high (see Figure A).

Nowadays a more refined version called asymmetric or double-key cryptography is much used. Here two related keys are generated, one of which is kept secret (S) and the other is made public (P). These two keys are generated using specific programs which start from a random number and it is practically impossible to deduce S from a knowledge of P and vice versa (provided the keys have been generated correctly).

Figure A
SYMMETRIC CRYPTOGRAPHY


"Hello, Michael"
CIHJT UUHML FRUGC ZIBGD BQPNI PDNJG LPLLP YJYXM
DCXAC JSJUK BIOYT MWQPX DLIRC BEXYK VKIMB TYIPE
UOLYQ OKOXH PIJKY DRDBC GEFZG UACKD RARCD HBYRI
DZJYO YKAIE LIUYW DFOHU IOHZV SRNDD KPSSO JMPQT
MHQHL OHQQD SMHNP HHOHQ GXRPJ XBXIP LLZAA VCMOG
AWSSZ YMFNI ATMON IXPBY FOZLE CVYSJ XZGPU CTFQY
HOVHU OCJGU QMWQV OIGOR BFHIZ TYFDB VBRMN XNLZC
"Hello, Michael"

SOURCE: Devised by author.

Asymmetric cryptography can be compared with a lock which has two keys: encryption (locking) by means of S can only be decrypted (unlocked) by means of P, and vice versa (see Figure B).

Asymmetric cryptography is usually combined with a certification authority which verifies the identity of a person when she generates and communicates her key pair. This person has to keep her private key secret, whereas the public key is readily accessible to all participants.

Asymmetric cryptography assures confidentiality in communications and allows the issuer of a message to be authenticated.

Confidentiality: suppose a person (Alice) wants to send an encrypted message to someone (Bob). Alice encrypts the message using the public key of Bob, so only Bob can decrypt it with his private key. Note that, unlike in classical or symmetric cryptography, there is no need for Alice and Bob to previously exchange their cryptographic keys.

Authentication or electronic signature: suppose that Alice wants to prove that she wrote a message. To do this, she sends the message to another person and attaches a copy of it encrypted using her secret key. The recipient uses Alice's public key to decrypt the encrypted message and compares it with the unencrypted information. If they are equal, it is clear that only Alice could have sent the message.

Another tool useful for understanding how Bitcoin works is the **hash function.** It is a cryptographic function (H) which, given an input x (any text or value of variable length), returns an output h (denoted "digest" or "hash") of fixed length (H(x)=h). Hash functions have the following properties:

- It is "trivial", given an input x, to find its hash h.
- It is "impossible", given h, to find x (one-way function).
- It is "impossible" to change x without changing h. Small changes in x return completely different outputs h.
- It is "impossible" to find two x which return the same h.[1]

Hash functions have many uses:

They can be used to increase **security.** A business may decide to store the hashes of its customers' passwords, instead of the passwords themselves. Thus, when a user types her password x, the business calculates the h hash (a trivial process) and compares it with the stored hash. If they coincide, the user can proceed with her purchase. A hacker who steals the information stored by the business only get the hashes of the users' passwords, which do not give him access to the passwords (x cannot be obtained from h).

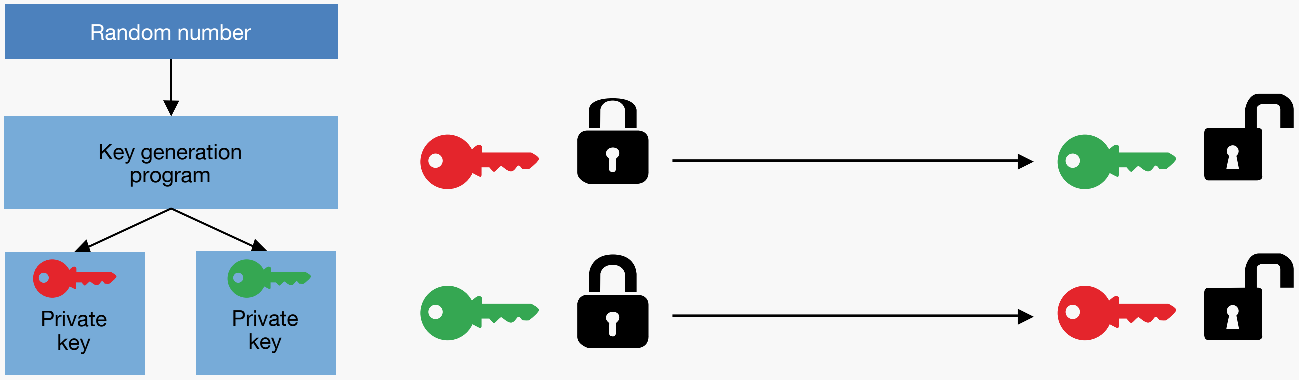
They can be used to **verify the integrity of information.** To do this, the hash of a message before it is sent is compared with that generated at the destination. If any change has been made, the hashes will be different, and comparing two hashes is simple because their size is limited.

They can also be used as a **summary or "digital fingerprint"** of a very extensive input.

They can also be used to **construct proof-of-work,** which are widely used in Bitcoin and which also have other applications, such as hindering denial-of-service attacks. Let us consider a

[1] "Trivial" means that very small amount of computing resources is required. "Impossible" is used to indicate that the computing power required to find a solution makes the process impracticable. For example, if we have a function H which gives a hash of 256 bits (such as SHA-256, used in Bitcoin), the task of finding two x's which give the same h requires an average of 2128 attempts. A computer which calculates 10,000 hashes per second would take 1027 years to find them (Nayaranan et al., 2016).

Figure B
ASYMMETRIC CRYPTOGRAPHY



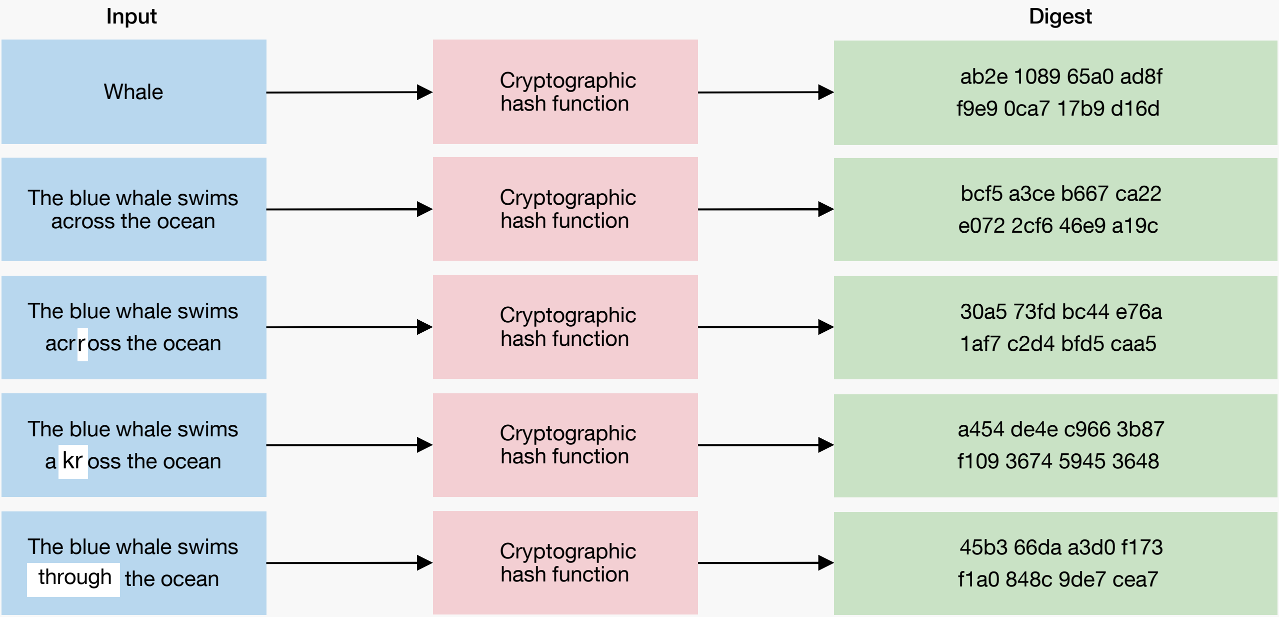
SOURCE: Devised by author.

business with its website. Each customer that visits the website triggers a series of requests (access to the catalogue, orders, queries) which the business's IT system has to deal with. An attacker could try to swamp the business's website with requests from different IP addresses to the point of blocking its service. To make this more difficult, the business may propose the resolution of an artificial problem (a cryptographic puzzle) each time it receives an access request. This simple problem would not pose much difficulty to a genuine user, but resolving a large number of small problems would be difficult for an attacker launching a massive number of requests.

A possible proof-of-work would be: "given a random x, find a value n (usually called "nonce" or single-use random number) such that H(x+n) is a hash beginning with four zeros". This calls for partially reversing a hash function (many H(x+n) expressions begin with four zeros). Finding the answer involves a trial and error process which uses up resources. The difficulty can be adjusted by changing the number of zeros (the more zeros, the greater the difficulty).

These basic concepts are sufficient to get a rough idea of how Bitcoin works.

Figure C
HASH FUNCTION


Input
Digest
Whale
Cryptographic hash function
ab2e 1089 65a0 ad8f f9e9 0ca7 17b9 d16d
The blue whale swims across the ocean
Cryptographic hash function
bcf5 a3ce b667 ca22 e072 2cf6 46e9 a19c
The blue whale swims acrross the ocean
Cryptographic hash function
30a5 73fd bc44 e76a 1af7 c2d4 bfd5 caa5
The blue whale swims akross the ocean
Cryptographic hash function
a454 de4e c966 3b87 f109 3674 5945 3648
The blue whale swims through the ocean
Cryptographic hash function
45b3 66da a3d0 f173 f1a0 848c 9de7 cea7

SOURCE: Own elaboration.

2.1 *Objective of Bitcoin*

Before beginning to construct a scheme like Bitcoin from scratch, we first have to specify what our objective is. This is best done by consulting the paper by Nakamoto (2008) which gave birth to the scheme. It begins by explaining that commerce on the internet relies on the intermediation of third parties (banks and other financial intermediaries) trusted by those participating in the transaction. According to Nakamoto, this model has some limitations. The first is that truly irreversible payments do not exist, since the intermediaries cannot avoid having to mediate between the parties in the event of disputes. The second problem, derived from the first, is that the intermediaries introduce a cost which makes small casual payments impractical. What is needed, according to Nakamoto, is *"an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party".* Thus our task is to create an electronic payment system similar to cash which allows remote payments without the need for a financial institution. Nakamoto considers that this would enable truly irreversible payments and would reduce intermediation costs.

2.2 Constructing Bitcoin

2.2.1 TESTCOIN VERSION 0

Now that the objective is clear, to get an idea of what an initial, very simple cryptocurrency scheme (let's call it testcoin) might be, we consider the sending of an internet message between the two parties. If Alice wishes to pay Bob, she could simply send him the following message: "I, Alice, wish to pay Bob 3 testcoins of the 20 that Charlie sent me yesterday".

Obviously this model has serious problems. Even assuming that the testcoins "sent" in the message have intrinsic value, there are many unresolved details: How does Bob know whether Alice received 20 testcoins from a third party called Charlie yesterday? How can he be sure that Alice has not sent similar messages to others to spend her testcoin balance several times over? How can Bob be sure that the content of the message has not been modified in transit and really reflects what Alice wanted to say? Finally, how can he be sure that Alice and not someone else sent him the message?

2.2.2 TESTCOIN VERSION 1

Although it is not the main problem of version 0 of the scheme, the latter problem is the easiest to solve. If Alice uses public-key cryptography,[2] she can sign the message with her private key and anybody could use Alice's public key to check that only she could have written the message.[3] It is possible to go further: taking into account that the objective is to replicate a remote payment system with properties similar to those of cash, it is not really important to Bob that Alice is actually Alice, but just that she has the money she is giving him. There is no need for Alice to really care who Bob is. In view of this, testcoin balances could be associated with the public keys of Alice and Bob, who do not need to exchange details on their identity. Thus, public keys would function as account numbers to which we can associate testcoin balances, such accounts not being associated with a specific identity.[4]

After these modifications, the message which could be sent in the revised version of the scheme (version 1) would be similar to the following:

> "I, public key 008646BBFB7D, send 3 testcoins associated with said key to
> public key 3FD8C0A9C6FF"

[2] See Box 1 for a brief, non-technical explanation of asymmetric cryptography and public keys for ensuring message confidentiality and authentication.

[3] In this case a trusted certification entity would be needed to verify the identity of Alice when she generates her keys.

[4] Since the identify of participants does not have to be guaranteed when the keys are generated, a certification entity is not necessary; users can generate as many key pairs ("accounts") as they wish using standard applications.

Alice would sign the message using the private key associated with her public key so that Bob (or anyone else) can check that only the person whose public key is 008646BBFB7D could have written the message.

Version 1 of the protocol looks better that the initial one. Alice and Bob only reveal their public keys, and Bob is sure that only the owner of the source account could have sent that message. However, the main problems besetting the initial version of the scheme persist: How can Bob be sure that the issuer actually has in her account the testcoins she sends? Even granting that she has them, how can Bob be sure that the issuer is not sending a similar message to various people to spend the same testcoins several times over?

This latter problem, known as double spending, has traditionally been the greatest obstacle facing this type of decentralised electronic payment systems. Given that the asset exchanged is digital, there is nothing to prevent the issuer from making as many perfect copies of it as wished and using them to pay several recipients. Since the asset is easily replicated, it will lack value. The usual way to prevent double spending is to interpose a trusted third party who verifies the transactions. This intermediary would receive Alice's message to Bob, verify that Alice's account has a sufficient balance and debit her account and credit his account. If Alice sends the testcoins to various recipients, the intermediary would reject the transactions once the available balance was exhausted. In short, the usual solution to the double-spending problem is to introduce a bank, which is precisely what we want to avoid.

2.2.3 TESTCOIN VERSION 2

At this point Nakamoto departed from traditional practice. Since a scheme in which the information is transmitted only between the two parties to a transaction does not work, and since the scheme wants to avoid a single intermediary in whom the parties have to trust, an alternative approach is needed. Nakamoto's solution is to retain the intermediary, but in a decentralised form. In other words, the scheme is designed so that all its members know all the transactions which have taken place and approve or reject them collectively.

Thus, in version 2 of the scheme, all users have a full copy of the ledger containing all the transactions which have taken place. Alice could send to Bob a message like that described in version 1 and Bob would use the transaction history to check that: (i) Alice actually received in a previous transaction the testcoins she is sending him and that (ii) she has not spent them since. Bob would add the new transaction to the ledger and share it with other network users so that they can update their copy.

However, this version of the scheme does not eliminate the possibility that Alice may try to double spend. Alice could send almost simultaneously two similar messages transferring the same testcoins to Bob and to Charlie. Bob and Charlie's checks would show that both transactions are possible according to their copies of the ledger, they would add them to the ledger and would share their (different) versions of the ledger with other users. This source of inconsistency would make it practically impossible to maintain a unified version of the ledger among the scheme participants.

2.2.4 TESTCOIN VERSION 3

To resolve this problem, we turn to version 3 of the protocol which introduces a change in the verification method. Instead of letting Bob or Charlie verify the transactions individually and disseminate potentially different versions of the ledger, the verification has to be done jointly by all users. Thus, when Alice sends the message to Bob, he does not check it on his own, but rather publishes it on the network so that all users know that Alice (they only actually know her public key) wants to send some testcoins to Bob (who is also only known by his public key). Bob will invite all users to decide whether or not the transaction is correct and should be entered in the ledger. If Alice tries to pay Bob and Charlie almost simultaneously, the network users will realise that the two transactions are incompatible and will choose which one should be entered in the ledger and which should be rejected, ensuring at all times that the ledger remains unique.

At first sight, this change looks promising, but it leaves some loose ends. The main one is agreement between participants: how can it be ensured that the scheme participants agree on which transactions may be entered in the ledger and which may not? Perhaps the simplest way of resolving the problem is by vote, granting one vote to each network participant, with those transactions receiving a majority vote being entered in the shared ledger. This approach has a fundamental problem, namely that it is relatively easy to construct a large number of false identities and attempt to deceive the network. Alice could (at a moderate cost) flood the network with fictitious identities voting in favour of entering in the ledger the payments to both Bob and Charlie, deceiving both of them and accepting as valid an inconsistent ledger entry.

2.2.5 TESTCOIN VERSION 4

To resolve the problem of agreement between the network actors, we have to turn to version 4 of the scheme, which is where Nakamoto makes his main, and probably least intuitive, innovation. To prevent a dishonest actor from deceiving the system with a large number of false identities, the process of approving transactions is made artificially difficult by what is known as a proof-of-work. In this way, the transaction history accepted by the scheme participants will not be that receiving most votes (votes are easy to falsify), but that entailing most computational work. Naturally, the participants have to be given an incentive to do this work, which uses up resources in the form of electricity and investment in hardware. Hence, verification will be remunerated by the assignment of recently created testcoins. We describe this procedure below in more detail.

When Alice wants to send her payment to Bob, the message is published for all participants, along with other prospective transactions for entry in the ledger. The participants have access to the transaction history, so they can verify at virtually no computational cost whether this group of new transactions (called a “block” of transactions) is consistent with past ledger entries. That is to say, a check is made that the issuers received funds previously and have not spent them and that the transactions being verified in the block are compatible with each other and do not entail double spending. If the check is successful, that block of transactions can be added to the ledger.

Before it is entered in the ledger, however, a proof-of-work must be carried out. Specifically, it is required that some user find a value x (nonce) such that the result of finding the hash[5] of the information in the block (basically the list of transactions intended to be entered in the ledger plus the information in the header) and appending it to the nonce gives a value beginning with a certain number of zeros.

H (information in the block, nonce) = value beginning with n zeros

Where:

Information in the block = header + list of transactions

As explained in Box 1, the result of the hash function is not predictable, so finding the nonce involves computational work which can only be resolved by brute force: testing values of x at random until one meeting the required condition is found. The number n of zeros required at the beginning can be adjusted to make the work more difficult or less difficult for users wishing to act as transaction verifiers.

Hence the verifiers, known as miners, compete to find a solution to this artificial problem. When a miner finds a solution, he publishes it so that all users can check that it is correct, which is very simple.[6] Once the validity of the transactions (existence of balance and absence of double spending) and the validity of the solution to the proof-of-work have been verified, the miners include the block in the ledger and continue working on the generation of new blocks.

An important matter yet to be resolved is the order of transactions. The ledger we are building is essentially a list of transactions ordered chronologically, to which blocks of transactions are gradually added. The chronological order of the blocks is essential in order to know whether or not a transaction can be carried out. Therefore, each new block entered in the ledger includes a reference to the immediately preceding block. This reference can be easily obtained by inserting in each block header the hash of the previous block. This creates a *blockchain*.[7]

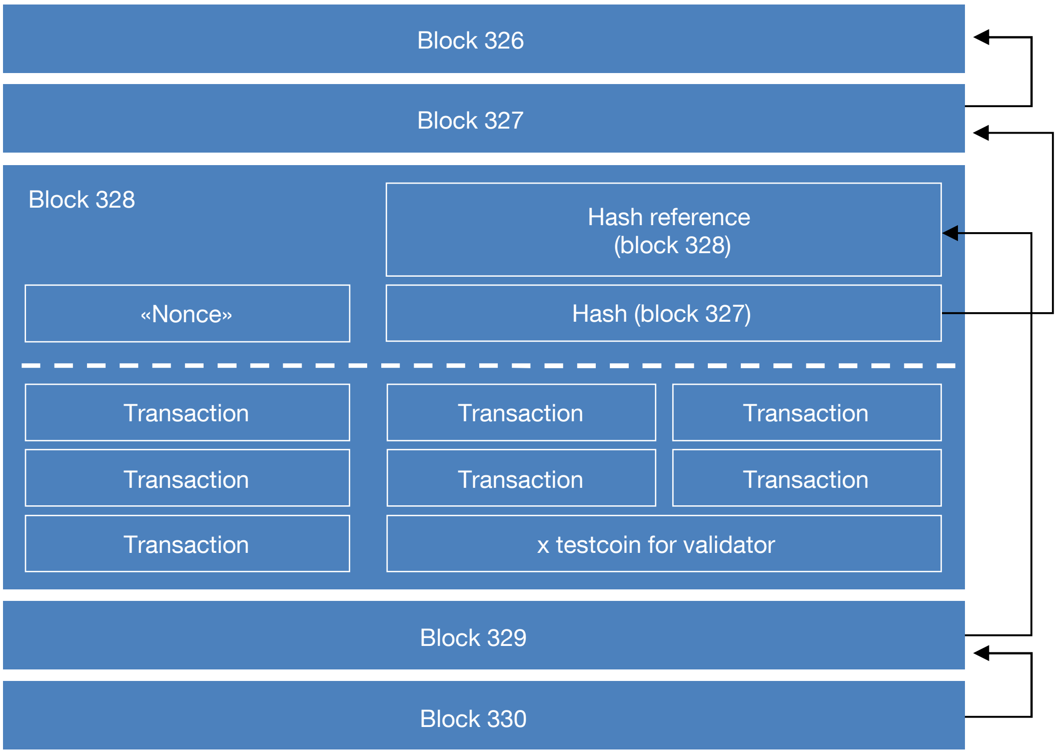
Finally, miners must be given an incentive to spend their time and money (purchase of hardware, electricity cost) searching for solutions to the proof-of-work. In this connection, each miner adds to the transactions in the block on which the proof-of-work is under way an additional payment in which that miner assigns himself a certain amount of testcoins. These testcoins do not come from any previous transaction, but rather are created as a reward for the work done to obtain the required nonce.

[5] For an elementary description of hash functions, see Box 1.

[6] It is very difficult to obtain a nonce x for which h (information in the block, x) has certain specific properties (e.g. beginning with n zeros). However, if x is known, it is very simple from a computational standpoint to find h (information in the block, x) and verify that the solution meets the required condition.

[7] The first, or genesis, block of bitcoin contained simply the headline of the Times of 3 January 2009 ("The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"), along with the assignment of 50 bitcoins for the miner who generated the block (presumably Nakamoto himself).

TESTCOIN BLOCKCHAIN FIGURE 2



SOURCE: Devised by author.

This is all that is needed. With some simplifications, testcoin version 4 reflects the basic functioning of the Bitcoin protocol. Figure 2 summarises the basic aspects of the blockchain we have just created.

Figure 2 describes from a practical standpoint the public-domain software which anyone can download from the internet and run on their computer to carry out transactions or attempt to verify them as a miner. There is no limit on entries into or exits from the network, which is completely unrestricted. In view of the current complexity of the proof-of-work, however, miners tend to be specialised professionals with purpose-designed IT equipment. Users do not normally participate directly in Bitcoin, but rather purchase their bitcoins in cryptocurrency exchanges (which sell cryptoassets for legal tender or act as intermediaries on a commission basis) and keep the keys of their bitcoins under custody in wallet applications or in specialised entities.

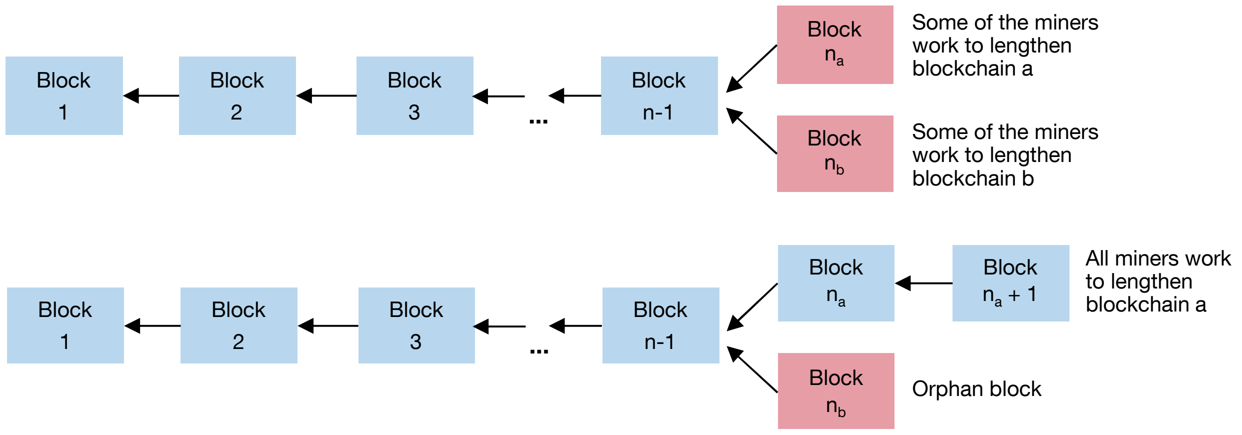
2.3 How does the ledger remain unique? Blockchain forks

Perhaps the first question which arises now that we have explained the basic functioning of Bitcoin, is whether a multitude of unknown verifiers spread across the world, lacking a relationship of mutual trust, is capable of keeping a unified transaction ledger. In reality, the ledger may have temporary branches or forks, as explained below.

The Bitcoin protocol determines that the longest linear blockchain (which is that containing most blocks and thus entailing a more demanding computational proof-of-work)

BLOCKCHAIN FORKS

FIGURE 3



SOURCE: Devised by author.

constitutes the correct version of the transaction ledger. Bitcoin is a global network with a multitude of nodes, so information exchange between nodes is not instantaneous. It could occur that virtually at the same time two validators find two valid solutions for the last block in the blockchain. Each validator will announce his solution to the other nodes and, considering the latency of the network, it is likely that the two solutions will be propagated unequally, with some nodes accepting solution n_a and others $n_{b.}$

The ledger will have forked into two blockchains of equal length, so the work of some miners will lengthen one blockchain and the work of the others will lengthen the other one. The near-simultaneous finding of solutions might be repeated, but in a short time some group of miners will generate a block for one of the two forks and communicate that solution to the whole network before a solution is found for the other fork. Let us suppose that the block n_a+1 is generated earliest; in that case, all the verifiers, regardless of the fork on which they were working, would see that the blockchain entailing most work is that with n+1 blocks. They would all move to the last block of that blockchain and work to lengthen it by generating block n_a+2. In this way consensus and ledger uniqueness are automatically restored.

Block n_b is called an orphan block and the transactions in it which are not yet included in the blockchain[8] return to “pending verification” status.

2.4 When can we consider that a transaction is final?

A consequence of the modus operandi described in the preceding section is the difficulty in precisely determining when a bitcoin transaction is deemed to have been executed. Returning to Figure 3 analysed in the preceding section, let us imagine that a transaction was included in block n_b but not in n_a or n_a+1. The beneficiary would believe that her transaction has been

[8] When blocks n_a and n_b were generated, the validators who generated them chose the transactions they included in the block of pending transactions. It is thus possible that some (or all, or none) of the transactions that were included in block n_a are also contained in block $n_{b.}$

included in the blockchain when actually it has only been included in a fork which has ceased to form part of the transaction mainstream. Once it is confirmed that block n_b is an orphan, the transaction returns to "pending confirmation" status. In view of this, recipients are advised to wait until various blocks (at least five) are added to ensure that the transaction has been included in the mainstream of the blockchain. Thus, the irrevocability of the transaction is not obtained at a specific moment, but is rather a gradual process in which the certainty that it has occurred is not absolute or assured, but rather increases as blocks are added to the blockchain.

2.5 How can Bitcoin be protected against fraud?

It should be emphasised that the system, by its very construction, prevents the most direct fraud. For example, all transactions have to be signed using the private key associated with the issuer's account, which means that a verifier cannot introduce a fraudulent payment and directly appropriate a balance owned by another person and transfer it to an account under that verifier's control.

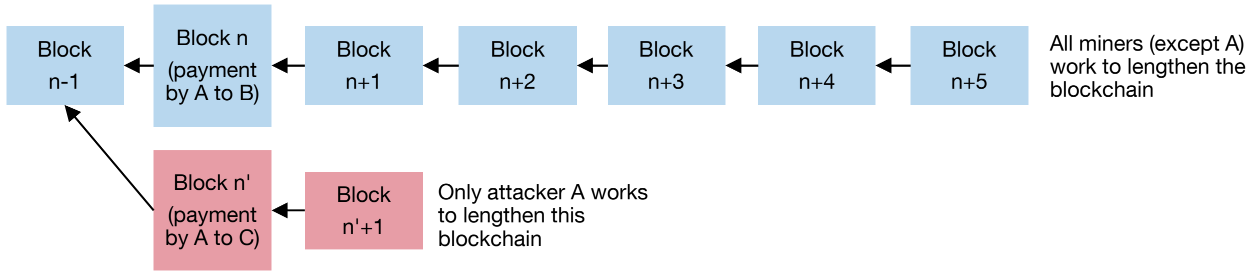
Nor can a verifier include a fraudulent transaction in a block (sending a higher balance than that available) or two mutually incompatible transactions (e.g. derived from sending the same balance to two different people). Even though the verifier in question may manage to find a valid nonce to generate the block, no other node would recognise it as correct in view of the transaction history, which is public.

However, other types of fraud are possible, although the system design makes their likelihood of success practically negligible. Specifically, let us consider the possibility of deceiving the system without infringing any rule. Imagine that Alice sends 10 bitcoins to Bob, the transaction is included in a block n and five additional blocks are added to the blockchain. When the blockchain reaches length n+5, according to the rule cited in the preceding section Bob declares that he is satisfied and confirms he has received payment. At that instant, Alice could devise an alternative block n (let us call it n') in which her payment to Bob is withdrawn and replaced by a payment to another public key controlled by Alice herself. If she were able to convince the other participants that node n' is correct and n is not, she would have managed to defraud Bob. In other words, Alice could attempt to alter the transaction history so as to undo a payment previously made by her and recover the funds.

To achieve that, Alice faces a number of difficulties. The first is to do the proof-of-work to find a nonce for block n', since changing a transaction alters the information in the block and so the previous nonce ceases to be valid. If Alice found the solution, she would not be able to convince the other miners that her blockchain (with n blocks, including the last, forged, one) is the correct one, since there is a longer blockchain with n+5 blocks. This latter blockchain contains more proofs-of-work, so the other miners accept it as correct. Alice could then try to insert block n' in the correct blockchain of n+5 blocks, but this is not possible because the pointer of block n+1 points to block n, not to n' (it is the hash of block n, not of block n'). Alice would have to change the pointer in block n+1 to the hash of n', but changing the information in block n+1, which becomes (n+1)' means

BLOCKCHAIN ATTACK

FIGURE 4


Block n-1
Block n (payment by A to B)
Block n+1
Block n+2
Block n+3
Block n+4
Block n+5
All miners (except A) work to lengthen the blockchain
Block n' (payment by A to C)
Block n'+1
Only attacker A works to lengthen this blockchain

SOURCE: Devised by author.

that the nonce of the block would cease to be valid, so the proof-of-work of block (n+1)' would have to be done, and so on repeatedly. In short, Alice would have to remake the blockchain on her own behalf (no miner wants to devote resources to mining blocks of such a short blockchain) and manage to make it exceed the length of the correct blockchain for it to be accepted by other participants. Meanwhile the other miners will prefer to lengthen the correct blockchain and try to get the related rewards. If Alice does not have more computational power than the other miners altogether, it is practically certain that the attack will fail. Not only would Alice not get near the length of the true blockchain, but she would progressively lose ground and nobody would recognise the transaction history proposed by her. She would be consuming resources in vain.

Instead of protecting the system from fraud through conventional security measures, Bitcoin opts to permit such undesirable acts (which do not infringe any rule of the system), but to disincentivise them through its very design. If Alice has less computational power than the other miners altogether, it is more profitable for her to cooperate with the system, generating blocks and obtaining rewards, than to confront it. If Alice has more computational power than the other miners together, the system is actually a centralised system and would lose its appeal to users.

2.6 Where are bitcoin balances stored?

The Bitcoin blockchain is essentially a chronological list of transactions. Consequently the question arises of where users' available balances are recorded. In order to understand the process which allows users to send and receive bitcoins and calculate the available balances, it is necessary to have a basic knowledge of the transactions recorded in the blockchain.

There are two types of transactions: the most common transactions have several inputs (balances received in previous transactions) and several outputs (balances sent to other recipients). The second type is the reward for miners which does not have inputs but does have an output in the form of bitcoins. This configuration allows users to send exact amounts, to pay fees, aggregate balances and receive change from a payment, as will be seen below.

Let's assume that Alice is a network user and received a balance of 5 bitcoins in transaction t_1, a balance of 3 bitcoins in transaction t_2 and a balance of 1 bitcoin in transaction t_3.

These balances were the outputs of those transactions and are associated with three accounts (public keys) whose password (associated private key) is only known by Alice. So far Alice has not made any payment but now she would like to pay Bob 2 bitcoins and Charlie 4 bitcoins. Also, as an incentive for the processing of the transaction, she would like to include a fee of 0.1 bitcoins for the miner who includes the transaction in a block.

In order to perform these transactions, Alice constructs transaction t_4 where the amounts received in transactions t_1 and t_2 (5 and 3 bitcoins) are included as inputs and the payments to Bob (2 bitcoins), to Charlie (4 bitcoins) and the "change" from the payment (1.9 bitcoins) are included as outputs. Alice sends the change to a new public address which she controls. The remainder (0.1 bitcoin) is the fee of the miner that includes the transaction in the blockchain. Charlie signs the transaction using the private keys associated with the source accounts (t_1 and t_2) and sends the outputs to the public keys of the recipients.

If Alice wanted to check her balance, she would have to aggregate the funds she has received as an output at some point in time which she has not used subsequently as an input of a transaction. After performing transaction t_4, Alice's final balance (2.9 bitcoins) is calculated by adding together the balances received in t_3 (1 bitcoin) and t_4 (1.9 bitcoins). In short, balances are not recorded in the Bitcoin blockchain but they are constructed indirectly by aggregating the unspent balances received from the addresses (accounts) owned by a specific user. This procedure is called UTXO (unspent transaction output).

2.7 Some figures[9]

The Bitcoin scheme is currently very small in size from a quantitative standpoint. As has already been indicated above, the creation of bitcoins is associated with the generation of blocks, with the result that the new bitcoins are granted to the verifier who finds the solution to the proof-of-work. This reward was initially 50 bitcoins per block, but under the protocol it is halved every 210,000 blocks. Taking into account that a block is created approximately every 10 minutes,[10] under this rule the rate of block creation will decrease, with rewards being halved every four years. The reward is currently 12.5 bitcoins per block and approximately 17.5 million bitcoins have already been issued. If the creation rule is not modified in future versions of the protocol, it is estimated that a total of 21 million bitcoins will be issued in a process which will last until 2140.

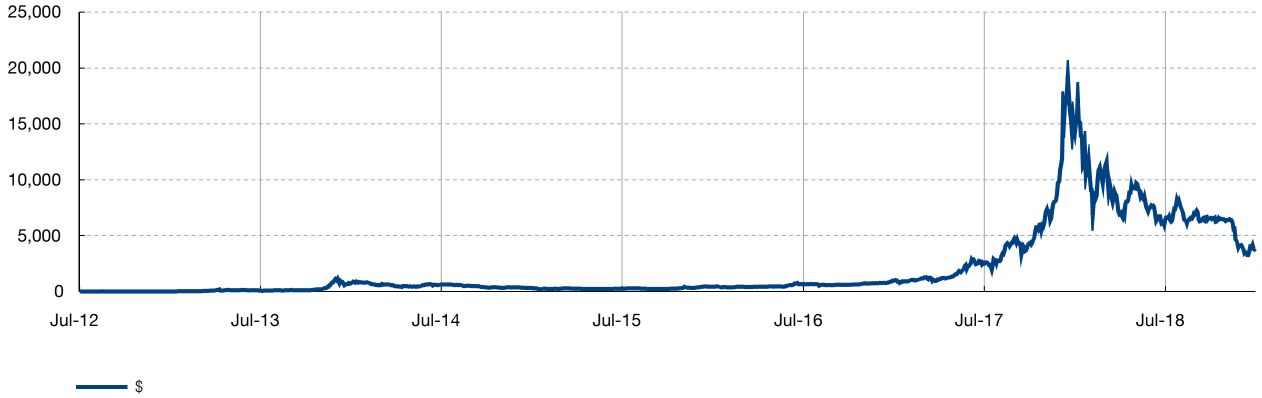
The price of bitcoins is very volatile. Following the tremendous rise in the latter half of 2017 (to just below $20,000 per bitcoin), its price experienced sharp swings as it fell notably (see Chart 1). At the end of 2018, its price was around $3,500 per bitcoin and, consequently, the approximate total value of bitcoins issued was nearly $60 billion.

[9] Figures obtained from www.blockchain.com (August 2018).

[10] The average rate of block creation remains constant since the Bitcoin protocol automatically adjusts the difficulty of the proof-of-work so that a block is generated every 10 minutes on average, irrespective of verifiers' computational power.

PRICE OF BITCOIN IN DOLLARS

CHART 1



SOURCE: https://www.blockchain.com.

The system processes approximately 250,000 transactions per day involving an estimated 150,000 bitcoins in total[11] (around $600 million). These figures are insignificant if we compare them with traditional payment systems. By way of comparison, according to the "Memoria Anual sobre la Vigilancia de las Infraestructuras de los Mercados Financieros" (Banco de España, 2018), the main Spanish retail payment system (the National Electronic Clearing System - SNCE by its Spanish abbreviation) processed a daily average of around 7.2 million payments amounting to approximately €7 billion. The SNCE essentially provides services to individuals and non-financial corporations in a country with 46 million inhabitants, whereas Bitcoin is a global scheme.

[11] Estimates constructed by deducting the amounts of change returned to issuers. This estimate includes purchases and sales of bitcoins in exchange for fiduciary currency and the purchase of goods and services as well as other transactions without a clear economic significance (e.g. the transfer of balances between addresses controlled by the same user).

3 Is Bitcoin a good payment system?

Leaving aside the strictly monetary aspects of bitcoin (its use as a unit of account, a medium of exchange or a store of value), this section focuses on the functioning of the Bitcoin blockchain as an alternative mechanism of exchange to traditional payment systems. Taking into account that Bitcoin was created for e-commerce and making casual payments over the internet (Nakamoto, 2008), it seems reasonable to centre the analysis on retail payment transactions.

The criteria used to assess Bitcoin as a retail payment system will be as follows: security, speed, cost, privacy, scalability, efficiency and business model sustainability over time.

3.1 Security

The advocates of Bitcoin present its security as one of the scheme's strengths. The transaction history is very reliable owing to the chaining of blocks using cryptographic techniques and it is practically impossible to alter this history, unless a majority of miners collude to forge the blockchain. The security of the balances recorded in the blockchain is ensured through a system of public and private keys. Apparently contradicting this high level of security, are frequent news items about bitcoin theft.

To analyse this aspect, the security of the core of the scheme (the Bitcoin blockchain) needs to be separated from the security of the scheme as a whole, including wallet applications and cryptocurrency exchanges.

The backbone of Bitcoin is the blockchain which is the public ledger containing the complete transaction history. Considering that users' balances are determined indirectly through the unspent amounts received, the whole scheme is based on trust in the fact that the history of these transactions is unique and does not permit alterations. The cryptographic chaining of blocks means that any alteration to the blockchain is immediately detectable.

Does this mean that it is safe to use Bitcoin? Not necessarily, from the standpoint of final users. Even if the shared ledger is forgery-proof and the core of the system functions securely, users may experience theft (and, in fact, this happens frequently).[12] Since users are not identified and the system is decentralised, ownership of bitcoins is demonstrated through the possession of the private key associated with the address at which those bitcoins are stored in the blockchain. If users lose the private key associated with an address, they actually lose the bitcoins (which would continue to be recorded in the blockchain, but users would not be able to use them, rendering them useless). If attackers steal the private key, they may perform a transaction by sending the bitcoins of another user to an account controlled by them. As the private key identifies the owner of the bitcoins, the transaction corresponding to the theft would

[12] According to some estimates, 14% of total bitcoins and other cryptocurrencies issued could have been stolen from their owners (https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies).

be indistinguishable from any other transaction and is compatible with the correct functioning of the blockchain.

In principle, users can operate directly in the scheme without intermediaries, so they could safeguard their private keys. However, this requires IT knowledge which is not within all users' reach. In order to operate in the scheme, most final users trust digital wallet providers and cryptocurrency exchanges which safeguard their customers' keys as part of their services. The most well-known Bitcoin security incidents have taken place at this type of entities, which are located on the periphery of the scheme and act as an interface between the Bitcoin network and end users. These entities are not usually regulated or supervised and users frequently have no-one to turn to if their accounts are looted or the entity safeguarding their balances goes bankrupt. One of the most famous cases took place in February 2014 when Mt. Gox – a major firm engaged in exchanging bitcoins for legal tender – went bankrupt in obscure circumstances, leaving many users without their funds.

Set against this, payment transactions through traditional systems and bank accounts are offered by supervised institutions which are highly experienced in information security. Furthermore, in case of fraud, regulations protect users who can claim the repayment of lost funds, in excess of certain amounts, from the financial institutions.

3.2 Speed

Speed is often mentioned as one of Bitcoin's fundamental qualities compared with traditional payments through financial intermediaries, since Bitcoin supposedly allows a transaction to be performed, from beginning to end, in 10 minutes on average. However, this speed is not always achieved and needs to be qualified for several reasons.

First, the speed of the process depends on the fee included in the transaction: a transaction which includes very low or no fees may remain in the queue for a long time or never be processed. Second, once the transaction has been incorporated into the Bitcoin blockchain, recipients are recommended to wait until five blocks have been added to the chain to have some assurance that the funds are really in their possession. This additional delay (of approximately 50 minutes on average) is recommended to rule out the possibility that the block in which the transaction has been included does not finally turn out to be an orphan block in a branch of the blockchain that does not ultimately form part of the transaction history.

In short, the Bitcoin is not as fast as is sometimes indicated and the velocity of the process is relatively unpredictable. Although the swiftness of Bitcoin may be a comparative advantage in certain payment market segments, such as international payments through correspondent banking, it is not striking compared with payments made nationally. At present, it is possible to make payments more quickly using a centralised architecture and traditional financial intermediaries. For example, card payments offer users a virtually immediate payment experience and it is possible to make transfers immediately between bank accounts in a question of seconds via a mobile or using internet banking.

3.3 Cost

Initially, Bitcoin advocates argued that the network allowed free transactions, although a small amount could be included voluntarily as a fee. These fees were a donation to the miner who managed to include the transaction in a block and, therefore, provided a small incentive for the miner in question to prioritise the processing of that transaction (miners can choose the transactions that they include in a block and, consequently, will choose those including the highest fees).

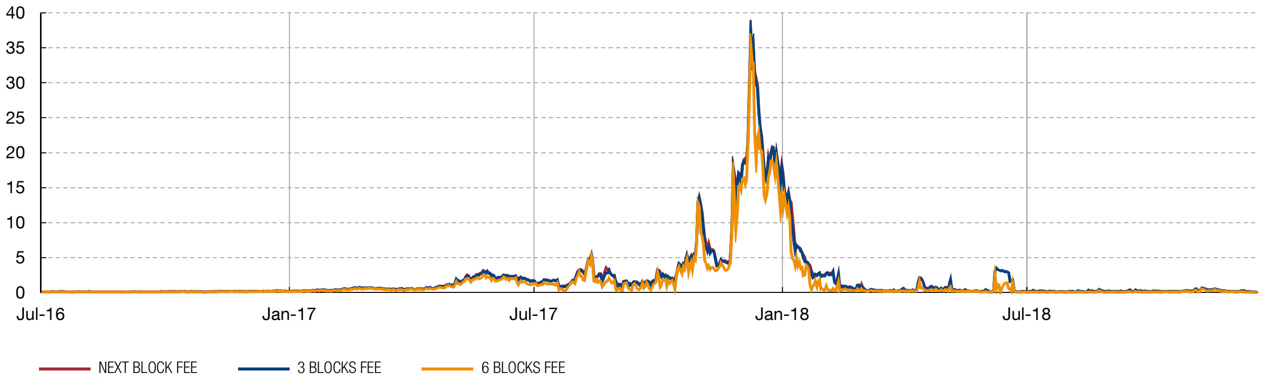
However, at present bitcoin transactions are subject to fees across the board. With the gradual rise in network traffic, the number of prospective transactions to be processed for inclusion in a block has increased significantly. Considering that the size of a block is limited (to 1 MB at present) and that the average rate of block production remains constant (approximately one block every 10 minutes), only transactions including fees are currently processed in a reasonable timeframe. Transactions with no fees remain in the queue indefinitely while sufficient numbers of transactions with fees for miners are entering the network. The minimum fee which ensures processing in a short lapse of time varies according to network traffic and logically tends to rise as traffic increases.

Certain bitcoin digital wallets include set fees per transaction by default (although their level can be parameterised by users), whereas other more modern wallets set a fee dynamically based on network traffic.

Fees essentially hinge on the size of the transaction and not on the amount transferred. Consequently, they tend to be relatively low for large payments and relatively high for micropayments (which is precisely the usage mentioned in the original report that led to the creation of the system). To give an idea of the order of magnitude, the minimum fees to ensure almost immediate processing of a normal size transaction were around $0.20 (December 2018) but climbed above $35 in December 2017 (coinciding with the tremendous appreciation of the bitcoin and an increase in the number of transactions in the network).

TRANSACTION FEES IN DOLLARS

CHART 2



SOURCE: https://bitcoinfees.info/.

In view of the gradual decrease in rewards for miners and the limit on memory set per block, any significant increase in network traffic will foreseeably cause fee spikes, unless substantial changes are made to the system's design.

Also, unless users want to hold a balance in bitcoins indefinitely, the cost of converting bitcoins into fiat money needs to be added to the fees directly related to the processing of transactions. This cost, which is rarely mentioned, can be substantial.

3.4 Anonymity and privacy

The Bitcoin scheme is presented as an anonymous payment system, despite being based on a public ledger. The personal information of participants in a transaction (names, account numbers, purpose of the payment) is normally transferred with the transaction message in traditional payment systems. All or part of this information is accessible to the issuer, the recipient and the intermediaries but not to unauthorised third parties. Bitcoin radically changes this approach since all the information on the transactions is public (basically, the account numbers and amounts), but data which may link an issuer or a recipient to a specific account are not included. Anonymity is compatible with the public nature of the blockchain and is presented as an advantage of Bitcoin, since the system can be used without supplying personal information that may be stolen.

Although the desire for anonymity may be for legitimate reasons,[13] this characteristic of Bitcoin has been criticised harshly by various authorities, especially considering that many intermediaries, which do not belong to the financial sphere, operate in this global network. As a result of the anonymity, it is difficult to apply measures to prevent money laundering and terrorist financing and, therefore, it is easy to use the system for transactions linked to unlawful activities. Perhaps the best-known case is that of the "Silk Road", a portal selling illegal substances and services hosted in the deep web which used precisely bitcoin as a means of payment. In October 2013, the FBI dismantled this portal, seizing 26,000 bitcoins.[14]

However, the alleged anonymity of Bitcoin is much lower than could be initially thought. Although the blockchain does not contain personal information, most users usually identify themselves to an intermediary[15] (for example, to a cryptocurrency exchange) the first time that they access the network and change real money into bitcoins (and, subsequently, when they sell the bitcoins in exchange for other currencies). Once users have bitcoins, they can use a limitless number of different accounts and split or combine their balances. Although transfers between the accounts of the same user are, in principle, indistinguishable from the transactions between

[13] For example, where users perform a transaction over the internet for the first time with a retailer with whom they do not have a relationship of trust, they could prefer to pay anonymously to avoid the retailer accessing their personal details (name, card number and expiry date) which may be used fraudulently later on if the retailer does not safekeep the information correctly.

[14] Their value at that time was $3.5 million. It was estimated that transactions amounting to $1.2 billion could have taken place over the two and a half years that the portal was in operation [see Halaburda et al (2016)].

[15] In the EU, for example, crypto asset exchanges are entities which must report to the authorities in order to combat money laundering and terrorist financing.

different users, since the ledger is public it is possible to perform a detailed statistical analysis of the transactions. As a result of this analysis, combined with other sources of information (for example, the identification of users when they change currency or the relationship between an account and an identity in a blog), the accounts of the same user can be identified in many cases and linked to a specific identity.[16]

3.5 Capacity

Bitcoin's current configuration puts a limit on the number of payments that can be processed by the scheme. If we take into account that the average rate of block production remains constant (10 minutes), that each block has a maximum size of 1MB and a typical network payment represents approximately 250 bytes,[17] a block could contain slightly more than 4,000 transactions, which represents some 7 transactions per second (or around 600,000 daily transactions). Although these figures are significant, the orders of magnitude are lower than those which are customary in current retail systems, especially considering that Bitcoin is a global network. As a reference, international card payment schemes are capable of processing thousands of transactions per second.

Actual network use was quite close to maximum capacity early in 2018 when transaction fees soared, coinciding with an increase in transactions and a rise in the price of bitcoin.

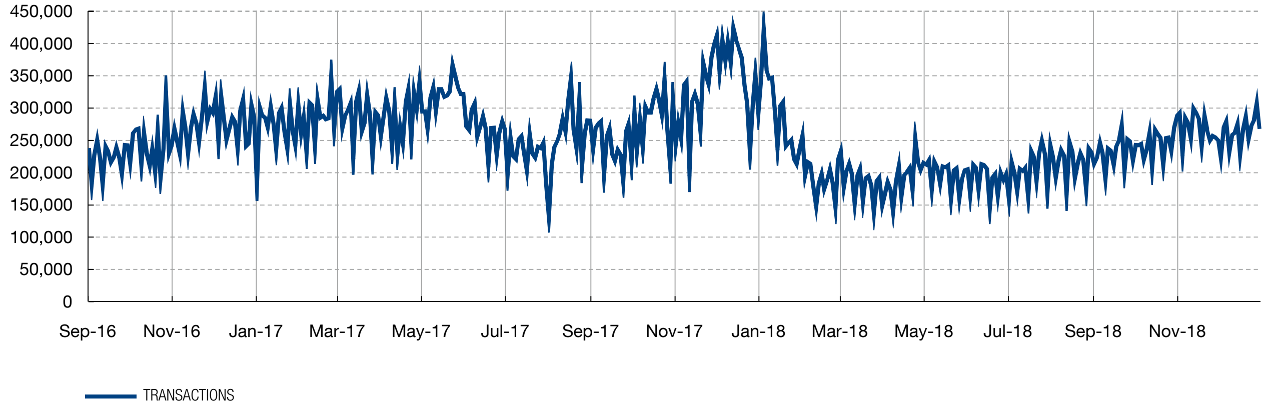
Modifications can be introduced to increase the capacity of the Bitcoin process, the most immediate of which would be to increase the maximum block size. However, it is not clear that a system based on a proof-of-work as demanding as that required by Bitcoin can be changed to process a significantly larger volume of transactions.

[16] Techniques and services also exist for "obscuring" the trail of funds and attempting to increase anonymity on the network (mixers).

[17] Source: https://bitcoinfees.info/.

NUMBER OF DAILY TRANSACTIONS

CHART 3



SOURCE: https://www.blockchain.com.

3.6 Efficiency and business model

The functioning of Bitcoin relies on the existence of miners who incur an expense (electricity and investment in hardware) to obtain income through transaction fees and the bitcoins which are created to reward miners who solve the cryptographic puzzle allowing blocks to be created. In principle, the difficulty of this cryptographic problem adapts automatically so that the rate of block creation is more or less constant. Despite some sporadic declines, the complexity shows a rising trend which is evidence of competition and increasingly specialised miners. This specialisation fosters the creation of miners' pools or clubs which combine their computational resources to increase their gains and reduce the variability in the rate at which they obtain rewards. The pooling of miners entails a process of centralisation: the four main miners' pools account for more than 50% of the whole network's computational power. This leads us to an oligopolistic business model in which the steep initial investment in specialised hardware could be an entry barrier to new actors. This model is far removed from the decentralisation which is usually attributed to Bitcoin.

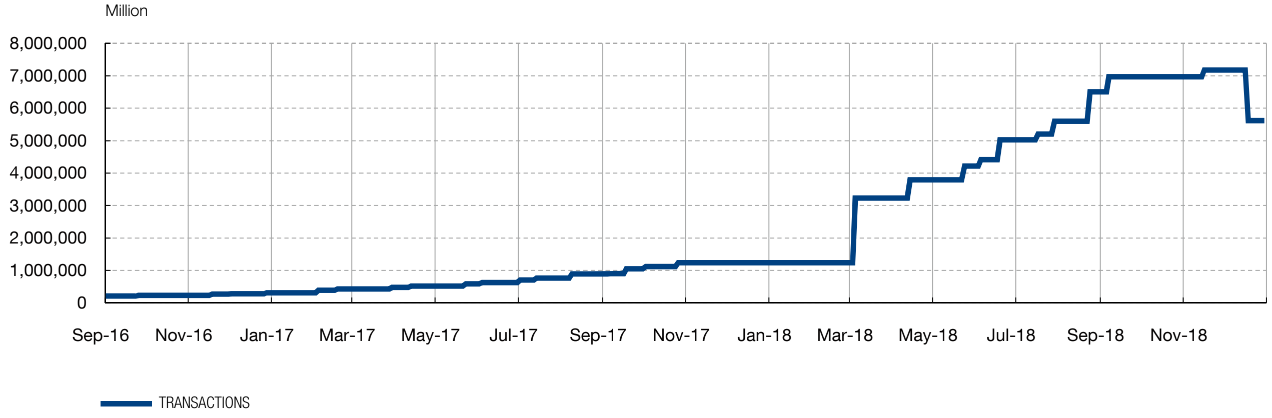
Aside from the number of miners, the complexity of the cryptographic validation process and the spending on resources which it entails, should be sufficient for calling into question the efficiency of a system which processes less than 300,000 daily transactions. As at August 2018 some estimates indicated that the Bitcoin scheme consumes 73.12 TWh, a similar amount of energy to that consumed by a country such as Austria.[18] In a trust-based centralised system, a similar volume of transactions could be processed with a negligible consumption of resources compared with Bitcoin.[19]

[18] Source: https://digiconomist.net/bitcoin-energy-consumption. This energy represents 0.33% of world consumption and would be enough to supply more than 6.7 million US households. The energy consumed in recording a single Bitcoin transaction could supply electricity to approximately 31 US households for one day.

[19] According to data from https://digiconomist.net/bitcoin-energy-consumption, the energy consumed in the verification of one Bitcoin transaction would be sufficient to process more than half a million VISA card transactions.

DIFFICULTY OF THE PROOF-OF-WORK

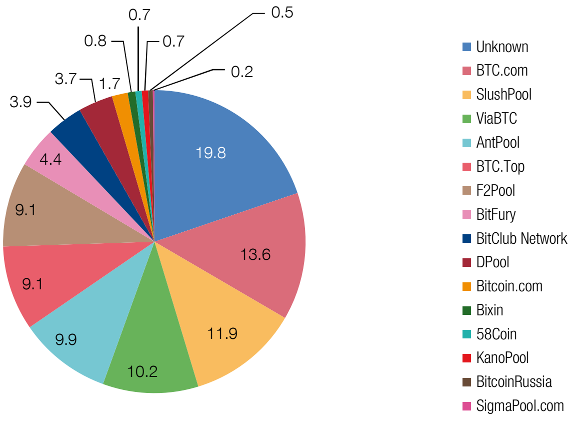
CHART 4



SOURCE: https://www.blockchain.com.

MARKET SHARE OF THE MOST POPULAR MINING POOLS (%)

CHART 5



SOURCE: www.blockchain.info.

This tremendous cost is currently covered by fees and through the issuance of new coins when blocks are created. As the automatic rewards decrease, if the difficulty continues to increase,[20] the fees will foreseeably rise to cover the scheme's huge electricity cost, which could call its viability into question. In late 2018 it became apparent how bitcoin price volatility may prompt changes in the number of miners. In this case, a drop in the equivalent dollar value of bitcoins caused a fall in the returns obtained by miners and a consequent exodus by them, which in turn gave rise to a decline in block generation and a resulting adjustment in difficulty.

3.7 Governance

An essential aspect of Bitcoin (which has been historically paid less attention than its technical characteristics) is governance. Bitcoin has typically been presented as an automatic protocol with immutable rules. Consequently, it is considered more trustworthy in certain circles than an authority such as a central bank, which can act discretionally by deciding the rate at which money is created and which transactions should be approved or rejected. However, the scheme is not immutable but evolves slowly provided that a critical mass of users agrees to implement changes. The maximum block size or the rule which determines that the rate of bitcoin creation will decline, could, for example, be changed at any time if enough users agreed to modify them. Significant change accepted by one part of the community of users but not by the other would lead the system to fork.[21]

The absence of a central authority, and the diversity and limited coordination of system actors make it difficult to reach agreements to gradually improve the system or react to unforeseen changes.

[20] See "Beyond the doomsday economics of "proof-of-work" in cryptocurrencies" for a detailed analysis of the long-term viability of Bitcoin.

[21] It was precisely the maximum block size (one of the most controversial aspects of Bitcoin, since this maximum size directly affects system capacity) that triggered the forking of Bitcoin into two mutually incompatible schemes (Bitcoin and Bitcoin Cash) since August 2017. There are many other versions of Bitcoin, although this name is usually reserved for the majority version.

4 Conclusions

Bitcoin is presented as an alternative to money and as a more efficient payment mechanism than traditional payment systems. In order to avoid the cost that intermediaries introduce into systems of exchange, Bitcoin pursues the creation of an alternative payment mechanism with no intermediaries that can censure transactions (understood as the ability to stop or reverse them).

It is essential to underline the scheme's ultimate objective since it influences its design, which is an almost natural response to the objective pursued [Brown (2016)]: taking into account that we want to make remote payments using a digital asset, we need validators to prevent users double spending and to verify the consistency of the transaction history; since we do not want a central authority to control the flow of payments, we must set up an open network where any party can act as a validator and the transaction history is public; given that all the transactions are public, we need them to be anonymous to guarantee confidentiality; to avoid one or several validators attempting to falsify the transactions ledger, they are required to compete to perform proof-of-work; and to provide an incentive for covering the cost of the proof-of-work, we set up a reward in the form of new monetary units. The details of how Bitcoin works can be found in section 2, but what is really important is to emphasize that the design is consistent with the objective pursued.

Bitcoin allows an uncensored payment system to be set up, which is a very interesting innovation that resolves a complex problem, but this does not necessarily mean that the scheme is a good payment system. The numerous advocates of Bitcoin argue that it represents an improvement to traditional payment transactions through the banking channel but these alleged advantages of Bitcoin do not seem to be supported by the information currently available.

Everything points to Bitcoin having serious shortcomings if it is intended for use as a large-scale payments system. The main problem is that the absence of intermediaries and the consequent decentralisation of the system through a set of validators who do not trust one another, leads us to a resource-intensive validation process which makes the system less efficient. In other words, there is a clear trade-off between the resource consumption linked to the decentralised validation of transactions and trust: as a result of centralised systems with an intermediary trusted by the parties involved, much simpler and more economic systems can be designed.

It is no surprise that Bitcoin has these problems. The scheme was not designed as an alternative to traditional payment systems but as a system "without a central authority with the power to authorise or reject transactions" (a system without the possibility of censorship). Bitcoin is an imaginative and elegant solution to this problem, but the commonly used payment systems do not seek to resolve this problem. The purpose of traditional payment systems is to make it easy to send money between any two actors in the simplest way possible, at a low cost, swiftly and with a high degree of security. These objectives are very different and, consequently, it is not at all surprising that Bitcoin does not function satisfactorily as a payment system (perhaps the opposite would be surprising).

Bitcoin detractors sometimes present it as a “solution in search of a problem”, whereas Bitcoin supporters believe it to be a solution to (what they believe are) the problems of fiduciary money and traditional payment systems. Bitcoin actually seems to be the solution to a problem, but to a different problem to that normally mentioned by its supporters: the creation of a system without censorship. Taking into account that for most agents the existence of trusted intermediaries is not a problem, along with the costs and inefficiencies generated when an attempt is made to eliminate these intermediaries, it does not seem that Bitcoin, as it currently stands, is going to have a significant impact for the financial sector as an alternative payment system to the traditional channels.

References

BANCO DE ESPAÑA (2018). *Memoria anual sobre la vigilancia de las infraestructuras de los mercados financieros, 2017.*

BANK OF INTERNATIONAL SETTLEMENTS (2019). *Beyond the doomsday Economics of "proof-of-work" in cryptocurrencies.* https://www.bis.org/publ/work765.pdf.

BROWN, R. G. (2016) *Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services* (https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/).

HALABURDA, H. and M. SARVARY (2016). *Beyond Bitcoin: The economics of digital currencies. Palgrave MacMilllan.*

https://bitcoinfees.info/.

NAKAMOTO, S. (2008). *Bitcoin: a peer to peer electronic cash system.*

NAYARANAN, A., J. BONNEAU, E. FELTEN, A. MILLER and S. GOLDFEDER (2016) *Bitcoin and cryptocurrency technologies.*

NIELSEN, M. (2013). *How the Bitcoin protocol actually works. (http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/).*

www.Blockchain.com.

BANCO DE ESPAÑA PUBLICATIONS

OCCASIONAL PAPERS

1201 ELOÍSA ORTEGA and JUAN PEÑALOSA: The Spanish economic crisis: key factors and growth challenges in the euro area. (There is a Spanish version of this edition with the same number).

1202 MARÍA J. NIETO: What role, if any, can market discipline play in supporting macroprudential policy?

1203 CONCHA ARTOLA and ENRIQUE GALÁN: Tracking the future on the web: construction of leading indicators using internet searches. (There is a Spanish version of this edition with the same number).

1204 JOSÉ LUIS MALO DE MOLINA: Luis Ángel Rojo en el Banco de España.

1205 PABLO HERNÁNDEZ DE COS and CARLOS THOMAS: El impacto de la consolidación fiscal sobre el crecimiento económico. Una ilustración para la economía española a partir de un modelo de equilibrio general.

1206 GALO NUÑO, CRISTINA PULIDO and RUBÉN SEGURA-CAYUELA: Long-run growth and demographic prospects in advanced economies.

1207 IGNACIO HERNANDO, JIMENA LLOPIS and JAVIER VALLÉS: Los retos para la política económica en un entorno de tipos de interés próximos a cero.

1208 JUAN CARLOS BERGANZA: Fiscal rules in Latin America: a survey.

1209 ÁNGEL ESTRADA and EVA VALDEOLIVAS: The fall of the labour income share in advanced economies.

1301 ETTORE DORRUCCI, GABOR PULA and DANIEL SANTABÁRBARA: China's economic growth and rebalancing.

1302 DANIEL GARROTE, JIMENA LLOPIS and JAVIER VALLÉS: Los canales del desapalancamiento del sector privado: una comparación internacional.

1303 PABLO HERNÁNDEZ DE COS and JUAN F. JIMENO: Fiscal policy and external imbalances in a debt crisis: the Spanish case.

1304 ELOÍSA ORTEGA and JUAN PEÑALOSA: Algunas reflexiones sobre la economía española tras cinco años de crisis.

1401 JOSÉ MARÍA SERENA and EVA VALDEOLIVAS: Integración financiera y modelos de financiación de los bancos globales.

1402 ANTONIO MONTESINOS, JAVIER J. PÉREZ and ROBERTO RAMOS: El empleo de las Administraciones Públicas en España: caracterización y evolución durante la crisis.

1403 SAMUEL HURTADO, PABLO MANZANO, EVA ORTEGA and ALBERTO URTASUN: Update and re-estimation of the Quarterly Model of Banco de España (MTBE).

1404 JUAN CARLOS BERGANZA, IGNACIO HERNANDO and JAVIER VALLÉS: Los desafíos para la política monetaria en las economías avanzadas tras la Gran Recesión.

1405 FERNANDO LÓPEZ VICENTE and JOSÉ MARÍA SERENA GARRALDA: Macroeconomic policy in Brazil: inflation targeting, public debt structure and credit policies.

1406 PABLO HERNÁNDEZ DE COS and DAVID LÓPEZ RODRÍGUEZ: Tax structure and revenue-raising capacity in Spain: A comparative analysis with the UE. (There is a Spanish version of this edition with the same number).

1407 OLYMPIA BOVER, ENRIQUE CORONADO and PILAR VELILLA: The Spanish survey of household finances (EFF): description and methods of the 2011 wave.

1501 MAR DELGADO TÉLLEZ, PABLO HERNÁNDEZ DE COS, SAMUEL HURTADO and JAVIER J. PÉREZ: Extraordinary mechanisms for payment of General Government suppliers in Spain. (There is a Spanish version of this edition with the same number).

1502 JOSÉ MANUEL MONTERO y ANA REGIL: La tasa de actividad en España: resistencia cíclica, determinantes y perspectivas futuras.

1503 MARIO IZQUIERDO and JUAN FRANCISCO JIMENO: Employment, wage and price reactions to the crisis in Spain: Firm-level evidence from the WDN survey.

1504 MARÍA DE LOS LLANOS MATEA: La demanda potencial de vivienda principal.

1601 JESÚS SAURINA and FRANCISCO JAVIER MENCÍA: Macroprudential policy: objectives, instruments and indicators. (There is a Spanish version of this edition with the same number).

1602 LUIS MOLINA, ESTHER LÓPEZ y ENRIQUE ALBEROLA: El posicionamiento exterior de la economía española.

1603 PILAR CUADRADO and ENRIQUE MORAL-BENITO: Potential growth of the Spanish economy. (There is a Spanish version of this edition with the same number).

1604 HENRIQUE S. BASSO and JAMES COSTAIN: Macroprudential theory: advances and challenges.

1605 PABLO HERNÁNDEZ DE COS, AITOR LACUESTA and ENRIQUE MORAL-BENITO: An exploration of real-time revisions of output gap estimates across European countries.

1606 PABLO HERNÁNDEZ DE COS, SAMUEL HURTADO, FRANCISCO MARTÍ and JAVIER J. PÉREZ: Public finances and inflation: the case of Spain.

1607 JAVIER J. PÉREZ, MARIE AOURIRI, MARÍA M. CAMPOS, DMITRIJ CELOV, DOMENICO DEPALO, EVANGELIA PAPAPETROU, JURGA PESLIAKAITĖ, ROBERTO RAMOS and MARTA RODRÍGUEZ-VIVES: The fiscal and macroeconomic effects of government wages and employment reform.

1608 JUAN CARLOS BERGANZA, PEDRO DEL RÍO and FRUCTUOSO BORRALLO: Determinants and implications of low global inflation rates.

1701 PABLO HERNÁNDEZ DE COS, JUAN FRANCISCO JIMENO and ROBERTO RAMOS: The Spanish public pension system: current situation, challenges and reform alternatives. (There is a Spanish version of this edition with the same number).

1702 EDUARDO BANDRÉS, MARÍA DOLORES GADEA-RIVAS and ANA GÓMEZ-LOSCOS: Regional business cycles across Europe.

1703 LUIS J. ÁLVAREZ and ISABEL SÁNCHEZ: A suite of inflation forecasting models.

1704 MARIO IZQUIERDO, JUAN FRANCISCO JIMENO, THEODORA KOSMA, ANA LAMO, STEPHEN MILLARD, TAIRI RÕÕM and ELIANA VIVIANO: Labour market adjustment in Europe during the crisis: microeconomic evidence from the Wage Dynamics Network survey.

1705 ÁNGEL LUIS GÓMEZ and M.ª DEL CARMEN SÁNCHEZ: Indicadores para el seguimiento y previsión de la inversión en construcción.

1706 DANILO LEIVA-LEON: Monitoring the Spanish Economy through the Lenses of Structural Bayesian VARs.

1707 OLYMPIA BOVER, JOSÉ MARÍA CASADO, ESTEBAN GARCÍA-MIRALLES, JOSÉ MARÍA LABEAGA and ROBERTO RAMOS: Microsimulation tools for the evaluation of fiscal policy reforms at the Banco de España.

1708 VICENTE SALAS, LUCIO SAN JUAN and JAVIER VALLÉS: The financial and real performance of non-financial corporations in the euro area: 1999-2015.

1709 ANA ARENCIBIA PAREJA, SAMUEL HURTADO, MERCEDES DE LUIS LÓPEZ and EVA ORTEGA: New version of the Quarterly Model of Banco de España (MTBE).

1801 ANA ARENCIBIA PAREJA, ANA GÓMEZ LOSCOS, MERCEDES DE LUIS LÓPEZ and GABRIEL PÉREZ QUIRÓS: A short-term forecasting model for the Spanish economy: GDP and its demand components.

1802 MIGUEL ALMUNIA, DAVID LÓPEZ-RODRÍGUEZ and ENRIQUE MORAL-BENITO: Evaluating the macro-representativeness of a firm-level database: an application for the Spanish economy.

1803 PABLO HERNÁNDEZ DE COS, DAVID LÓPEZ RODRÍGUEZ and JAVIER J. PÉREZ: The challenges of public deleveraging. (There is a Spanish version of this edition with the same number).

1804 OLYMPIA BOVER, LAURA CRESPO, CARLOS GENTO and ISMAEL MORENO: The Spanish Survey of Household Finances (EFF): description and methods of the 2014 wave.

1805 ENRIQUE MORAL-BENITO: The microeconomic origins of the Spanish boom.

1806 BRINDUSA ANGHEL, HENRIQUE BASSO, OLYMPIA BOVER, JOSÉ MARÍA CASADO, LAURA HOSPIDO, MARIO IZQUIERDO, IVAN A. KATARYNIUK, AITOR LACUESTA, JOSÉ MANUEL MONTERO and ELENA VOZMEDIANO: Income, consumption and wealth inequality in Spain. (There is a Spanish version of this edition with the same number).

1807 MAR DELGADO-TÉLLEZ and JAVIER J. PÉREZ: Institutional and economic determinants of regional public debt in Spain.

1808 CHENXU FU and ENRIQUE MORAL-BENITO: The evolution of Spanish total factor productivity since the Global Financial Crisis.

1809 CONCHA ARTOLA, ALEJANDRO FIORITO, MARÍA GIL, JAVIER J. PÉREZ, ALBERTO URTASUN and DIEGO VILA: Monitoring the Spanish economy from a regional perspective: main elements of analysis.

1810 DAVID LÓPEZ-RODRÍGUEZ and CRISTINA GARCÍA CIRIA: Estructura impositiva de España en el contexto de la Unión Europea.

1811 JORGE MARTÍNEZ: Previsión de la carga de intereses de las Administraciones Públicas.

1901 CARLOS CONESA: Bitcoin: a solution for payment systems or a solution in search of a problem? (There is a Spanish version of this edition with the same number).

BANCO DE ESPAÑA
Eurosistema

Unidad de Servicios Auxiliares
Alcalá, 48 - 28014 Madrid
E-mail: publicaciones@bde.es
www.bde.es