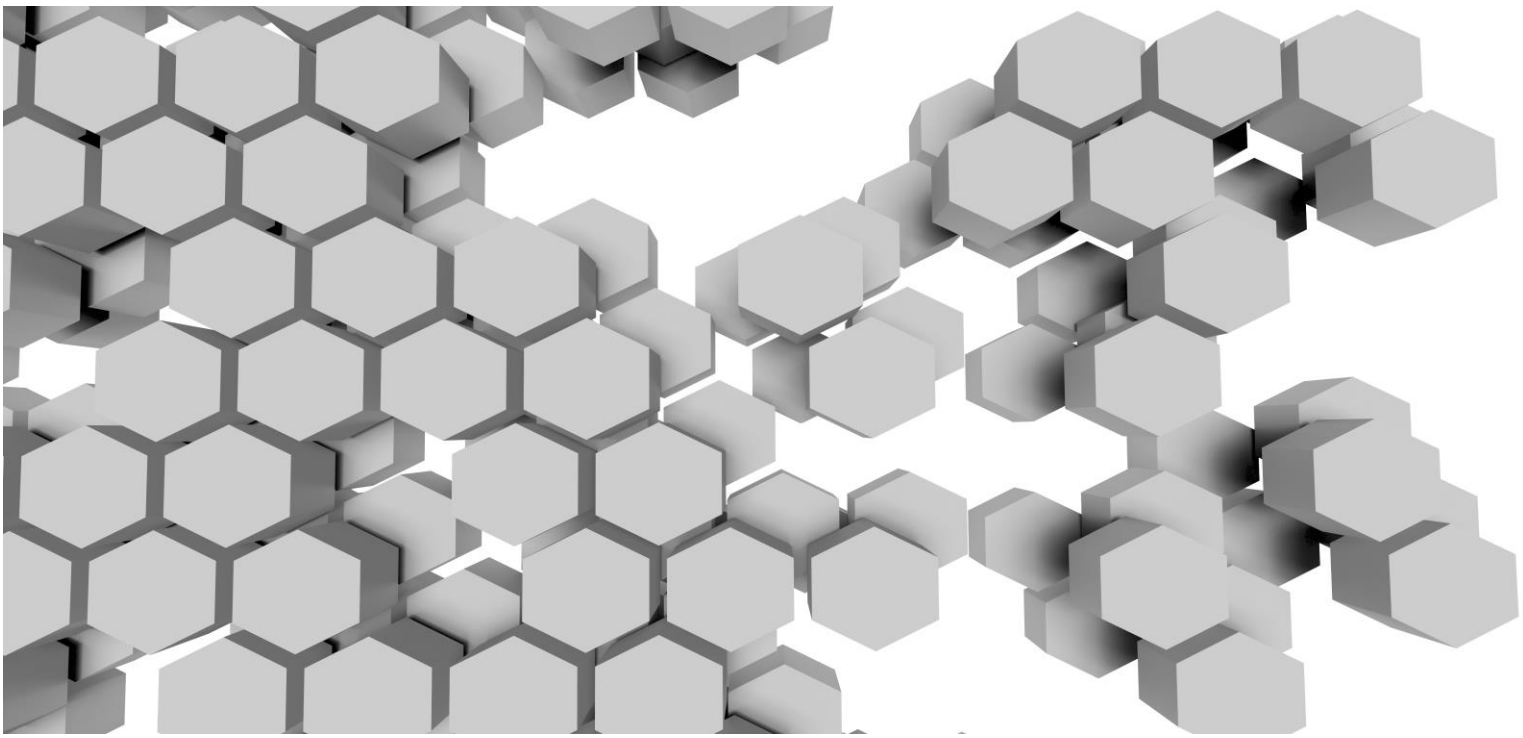
View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by JRC Publications Repository

European Commission

JRC TECHNICAL REPORT



Overview and Analysis of the Concept and Applications of Virtual Currencies

Author

Prof. Sead Muftic

Editors

Ignacio Sanchez, EC DG JRC

Laurent Beslay, EC DG JRC

2016

EUR 28386 EN

Joint Research Centre

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information

Laurent Beslay

Address: Joint Research Centre, Via Enrico Fermi 2749, 21027 Ispra, Italy

E-mail: laurent.beslay@ec.europa.eu

Tel.: +39 0332 78 6556

JRC Science Hub

https://ec.europa.eu/jrc

JRC105207

EUR 28386 EN

PDF	ISBN 978-92-79-64826-7	ISSN 1831-9424	doi:10.2788/16688
Print	ISBN 978-92-79-64825-0	ISSN 1018-5593	doi:10.2788/242242

Luxembourg: Publications Office of the European Union, 2016

© European Union, 2016

The reuse of the document is authorised, provided the source is acknowledged and the original meaning or message of the texts are not distorted. The European Commission shall not be held liable for any consequences stemming from the reuse.

How to cite this report: Muftic S., Ignacio Sanchez I. (ed.) and Beslay L. (ed.), *Overview and Analysis of the Concept and Applications of Virtual Currencies* , EUR 28386 EN , doi:10.2788/16688

All images © European Union 2016, except frontpage: © zapp2photo – Fotolia.com

Abstract

This Report is dealing with virtual currencies – their concept and applications. The Report starts with the description of different types of virtual currencies, first Bitcoin, then some other types of crypto currencies, followed by description of virtual currencies that are created by conversion of real–world currencies, and finally, virtual currencies based on different types of non–financial assets. The common characteristics of all types of virtual currencies and applications based on them is support for various types of financial transactions.

The analysis of the Bitcoin system includes its functional aspects, but also its weaknesses and problems. In addition to the Bitcoin and other popular systems using alternative virtual currencies for payment transactions, the Report also outlines some trends and current initiatives to use the concept of the public ledger – blockchain as support for validation and authorization of distributed, peer-to–peer financial transactions. Most of such current trends rely on use of the currently operational Bitcoin network and in that way they are directly vulnerable to the weaknesses and threats originating from that network.

Table of contents

List of Figures

Executive Summary

This Report is dealing with virtual currencies – their concept and applications. The Report starts with the description of different types of virtual currencies. Bitcoin is described first, then some other types of crypto currencies, followed by description of virtual currencies that are created by conversion of real–world currencies, and finally, virtual currencies are described that are based on different types of non–financial assets. The common framework of all types of virtual currencies and applications based on them considered in this Report is support for various types of financial transactions.

The analysis of the Bitcoin system includes its functional aspects, but also its weaknesses and problems. Functional aspects include the cycle of a payment transaction and components of the Bitcoin system that support it. The problems with Bitcoin are structured in three groups: the problems with the concept, the problems with the existing resources and deployments, and the problems with security and protection of system components and resources.

In addition to the Bitcoin and other popular systems using alternative virtual currencies for payment transactions, the Report also outlines some trends and current initiatives for the use of the concept of the public ledger – blockchain, as supporting infrastructure for validation and authorization of distributed, peer-to–peer financial transactions. Most of such current trends rely on use of the currently operational Bitcoin network and in that way they are directly vulnerable to the weaknesses and threats originating from that network.

The goal of this Report is to serve as the background document to support discussion of the possibilities or even cases where virtual currencies are the vector to conduct attacks and also the target of attacks. The purpose of the Report is to support the discussion regarding criminal activities where virtual currencies are the target from the perspective of the prosecution of those crimes, more than the protection against those crimes.

1 Introduction to the Bitcoin System

1.1 Introduction and General Description

There are many definitions and descriptions of the Bitcoin. Some describe it as an innovative currency, some as peer-to–peer electronic cash payments transactions, and some others as decentralized and anonymous payment system.

In this Report the Bitcoin system is treated as a payment system. It has its own features, its own currency, its own protocols and components, and with all that Bitcoin supports payment transactions. In other words, the core function of the Bitcoin system is to support payments between two parties – the party that makes a payment and the party that receives the payment. This approach is based on the description of the Bitcoin [Bitcoin, 2016], "*It is a decentralized digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority: transaction management and money issuance are carried out collectively by the network*".

The system is decentralized since users perform transactions within the community of registered users. Digital currency used in the system is not electronic form of real currency, but a special type of the currency generated and used only within the Bitcoin system. This concept is based on the notion that money can be interpreted as any object, or any sort of record, accepted as payment for goods and services and repayment of debts in a given country or socio-economic context. Bitcoin is designed around the idea of using cryptography to control the creation and transfer of money, rather than relying on central authorities.

There are several important requirements when making any type of payment and with any currency. The best example of a "perfect" payment transaction that meets all these requirements is payment in cash over-the-counter. When a consumer pays to a merchant using cash over-the-counter, such transaction satisfies all requirements and expectations of both parties. First, the transaction is *instantaneous*, as the paper bill is transferred hand-to-hand, from the consumer to the merchant. The transaction is *cheap*, in fact there is no overhead charge to perform transaction, so the merchant receives the full amount. The transaction is *irreversible*, what is beneficial to merchants. The transaction is *legal*, as the merchant can verify the legality of the paper bill. And, finally, the transaction is *anonymous* for the consumer as he/she does not need to reveal his/her identity in order to make payment.

The only "problem" with cash over-the-counter is the cash itself, as using and handling cash has many disadvantages.

Bitcoin concept and Bitcoin system solve all issues and problems with the use of cash, but at the same time provide all advantages when performing transactions using digital and communication technologies. So, paying with bitcoins is effectively a payment transaction equivalent to "digital cash" over-the-counter. Bitcoin system provides all advantages and benefits mentioned above with payments using cash over-the-counter, but eliminates the problems of using cash. That is the reason why bitcoins are often referred to as "digital cash".

One of significant features of payments using cash over-the-counter is that there are *no third parties* to participate or assist in the transaction. This feature makes execution of transactions very efficient and also very cheap to perform. Other types of todays payment systems, for instance using bank-to-bank account transfers or using bankcards, besides two transaction parties need many additional parties and use very complicated background infrastructure to validate and clear payment transactions. These infrastructures are complex to establish and

operate, they are expensive, and they are vulnerable to attacks and penetrations by hackers. Bitcoin does not use such complex infrastructures, what is the reason that its transactions are efficient and cheap. An additional problem with third-party transaction players is that transaction parties must put the complete trust in all these parties without any means to verify their functionality, correctness, or security. Finally, the problem with third parties is that payment transactions have no privacy of transaction parties.

Bitcoin system uses public-key cryptography to protect its currency and transactions. Logical relationships between transaction parties is direct, peer-to-peer, and the process of validating transactions is based on cryptographic proof-of-work. When performing a transaction, the net effect is that certain amount of bitcoins is transferred from one cryptographic address to another. Each user may have and may use several addresses simultaneously. Each payment transaction is broadcast to the network of distributed transactions processing servers. These servers collect individual transactions, package them into blocks, send them for validation, and distribute them after validation to all members of the Bitcoin system.

Each block is cryptographically processed by the large number of so called "miners". They each attempt to create cryptographic hash value which has special form. This is computationally very difficult and time-consuming task, therefore, it is very difficult to repeat. Individual blocks are validated using cryptographic processing procedures that require substantial amount of work and computing power.

Approximately an hour or two after submitting the transaction for validation, each transaction is locked in time and by cryptographic processing by the massive amount of computing power that was used to complete the block. When the block is validated, it is added to the chain of all previous blocks, thus forming a public archive of all blocks and transactions in the system.

One of the most important problems with uncontrolled digital currency, where there are no third parties to validate and approve transactions, is so called *double spending*. Since the currency is digital, stored on user's local workstations, in mobile phones, or on network servers, the same amount of currency can be easily copied and sent to multiple recipients multiple times.

Bitcoin system solves this problem with a very interesting approach. It is the first effective example of the solution for the double-spending problem without the need for assistance of any third party. Bitcoin solves this problem by keeping and distributing an archive of all transactions among all the users of the system via a peer-to-peer distribution network. Every transaction that occurs in the Bitcoin system is recorded in that public and distributed transactions ledger. Since the components in that ledger are blocks with transactions and the blocks are "chained" in time and in a cryptographic sequence, the ledger in the Bitcoin system is called *blockchain*.

That full blockchain of all transactions that were performed in the Bitcoin system before the specific transaction is used to verify validity of new transactions and to prevent double–spending. The transactions are verified against the blockchain to ensure that the same bitcoins have not been previously spent. This approach eliminates the double-spending problem. The essence of the verification procedure for a single transaction in fact is the test of the balance of the sending account. The test is very normal and natural: payment of a certain amount of the currency can be made only of the balance of the outgoing account is equal or larger than the payment amount. Current balance of an account is established by tracing all incoming and outgoing transactions for that account.

The procedure to verify validity of individual transactions and to prevent double-spending is based on the use of special type of cryptographic protocol called *public-key cryptography*. With this type of cryptographic systems each user has two cryptographic keys. They are mutually related in the sense that, what ever the one key encrypts, the other key decrypts. One of the two keys is a *private key* that is kept secret, and the other key is *public key* that can be shared with all other users in the system. When a user wants to make a payment to another user, the sender transfers certain amount of bitcoins from his/her account to the account of the receiver. This action is performed by the sender by creating a payment message, called a "transaction," which contains recipient's public key – receiving address and payment amount. The transaction is cryptographically processed by the sender's private key, the operation called *digital signing*, and as the result digital signature is created and appended to the transaction.

By using sender's private key every user in the system can verify that the transaction was indeed created by the indicated sender, as his/her private key can successfully decrypt the content of the digital signature. The exchange is authentic, since the transaction was also cryptographically processed with the recipient's public key, the operation called *digital enveloping*. This transformation guarantees that the transaction can be accepted and processed only by the holder of the corresponding private key, which is the intended recipient.

Every transaction, and thus the transfer of ownership of the specified amount of bitcoins, is inserted, then time-stamped, and finally displayed in one "block" of the blockchain. Public-key cryptography ensures that all computers in the network have a constantly updated and verified record of all transactions within the Bitcoin network, which prevents double-spending and fraud.

1.2 The Concept and Features

There are many concepts and even more operational payment systems today. Some are standard paper–based, some are digital and network based. What makes Bitcoin unique and distinctive, compared with all other payment systems in use today, are several of its core characteristics.

The first of them is that the system uses *its own currency*. The unit of the currency is called *bitcoin*. The currency is so called *crypto currency*, meaning that it is generated and used based on execution of certain cryptographic algorithms and protocols. Performing specific cryptographic protocols is in the heart of operations to create new bitcoins, to transfer them between transaction parties, and to validate the correctness of transactions.

The second interesting and important feature of the Bitcoin system is that the logical relationship between the two transaction parties is direct, *peer-to–peer*, i.e. there are no other parties that participate in the transaction. This is an important feature and benefit / advantage of the system that contributes to its efficiency when compared with the todays complex and expensive financial payment infrastructures and protocols. However, for distribution of transactions to their validators and later to all other members in the Bitcoin system the physical flow of each transaction is very complex and includes many parties.

The next important characteristic of the system is *anonymity of users*, their accounts, and transactions. This property means that the identities of the participants in the system are not known even to the partners performing a payment transaction. All other system operations – receiving payments, making payments, validating transactions, etc. are also performed anonymously. Interpreting this property correctly, the anonymity of transaction participants is

so called *pseudo-anonymity*. Namely, in the process of validating transactions, all previous transactions of the sender are traced back to the original initial transaction. If that initial transaction was the purchase of bitcoins at some Bitcoin Exchange, then the identity of the original owner of bitcoins is known.

Another very important feature is that the system is *not controlled* by any financial institution, by any regulatory body or by any legal financial authority. This means that the currency used in the system and all transactions are exempted from any legal and financial rules and regulations. The rules controlling Bitcoin system are built in its code. This property is usually called "*rule by the technical code*", as the rules of system operations, built in the code of its operational components, control and rule the operations of the system [UK, 2016, Chapter 3]. This property is sometimes described as "control by the community", i.e. by the users participating in the system.

1.3 Innovative Contributions of the Bitcoin System

Besides an effective procedure to transfer an amount of virtual currency from one user (account) to another user (account), the major and indeed an essential contribution of the concept of the Bitcoin is the solution to the general problem how to establish trust between two mutually unknown and otherwise unrelated parties to such an extent and certainty that sensitive and secure transactions can be performed with full confidence over an open environment, such as Internet. In all current large scale and not only financial systems that problem is solved by using the assistance of third parties. For many applications and transactions those third parties are integrated and linked into a large, complex, expensive and vulnerable operational infrastructures. Examples of such infrastructures today are the infrastructure to authorize and validate bankcard payments, the infrastructure that supports international financial transfers (SWIFT), Public–Key Infrastructures (PKI), various global Identity Management Systems, large and popular social Web sites, and many others. It is a general consent that such infrastructures are inefficient, expensive and, more important, vulnerable to external and internal attacks.

In addition to the complexity and vulnerabilities of such operational supporting infrastructures, another requirement and prerequisite to use their services is that users must put the complete trust in those third parties. Accepting to trust those third–party service providers is the necessary and mandatory prerequisite to use their services.

Therefore, one of the most important contributions of the concept of Bitcoin is that it solves the issue how two parties, mutually unknown to each other in advance and otherwise completely unrelated, can perform sensitive and secure transactions, such as transfer of money – payments, but without assistance of any third party and without the need to place trust in any component of the system.

The practical benefits of solving this problem and the most important consequence of this solution is that Bitcoin provides the possibility for one Internet user to transfer not only bitcoins, but also any other form of digital asset to or shared with another Internet user, such that the transfer is guaranteed to be safe and secure, that everyone knows that the transfer has been performed, and nobody can challenge the legitimacy of the transfer.

This feature of the Bitcoin system generated many very new, creative and innovative ideas where the concept equivalent to the Bitcoin can be used to perform secure and reliable transactions between users in an open community handling any type of digital asset ([Andreesen, 2014], [Sparkes, 2014], [UniCredit, 2016], [BitID, 2015], [PoE, 2015]). The examples of such applications and transactions range from commercial transitions, real estate

transactions, energy trading, electronic voting, medical applications, and many others ([Kounelis, 2015], [Muftic, 2016]). That is the main reason why the concept of blockchain, as technology supporting validation of all such transactions, is considered an innovative and disruptive technology.

2 Bitcoin Payment Transaction Cycle

In this chapter the complete cycle of one Bitcoin payment transaction, originating from its sender and terminating at its recipient, is described. The cycle comprises several consecutive steps explained in their chronological and functional sequence. In the course of these explanations, all outstanding questions and problems that were left unanswered in the previous chapter will be clarified.

The components participating in the full payment transaction cycle, the phases of the cycle, and individual steps are all shown in Figure 1. Individual steps are numbered, from (1) to (8), and each step is described in detail in the subsequent sections of this chapter.

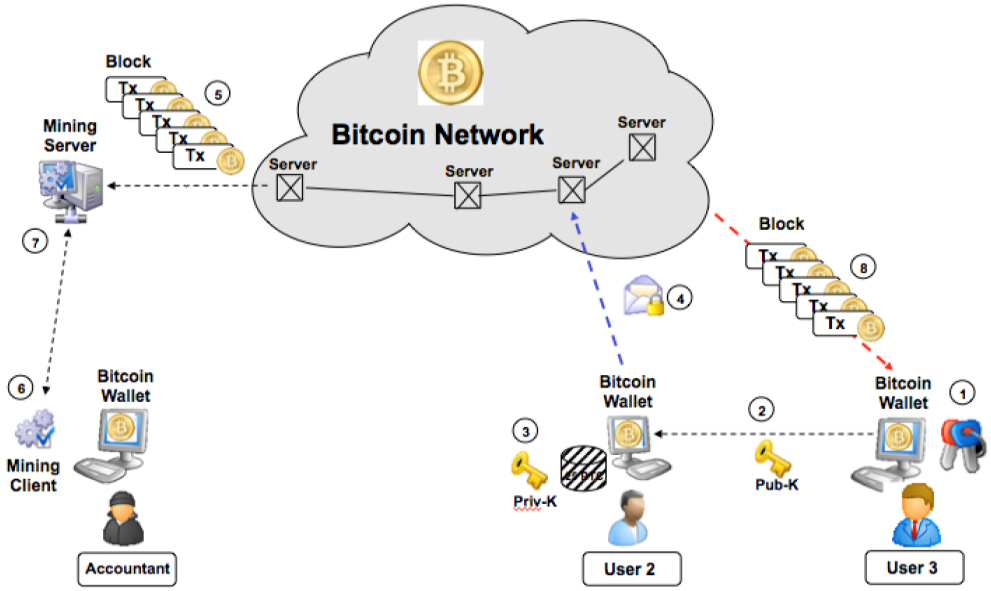


Figure 1. Bitcoin Payment Transaction Cycle

2.1 Generation of Bitcoin Addresses – Step (1)

Every user, in order to become the member of the Bitcoin system, must generate his/her Bitcoin address which is used to receive and make bitcoin payments and to keep the balance of unspent bitcoins. The core cryptographic apparatus in the Bitcoin system is based on public key cryptography. Cryptographic algorithms that support this type of cryptography use a pair of cryptographic keys – one is called *private key* and the other is called *public key*. These names indicate the essential rules of management of these keys: public keys are public, distributed to all other members of the system, while private keys must be extremely private and strongly protected, so that their use only by their owners is guaranteed.

In principle, cryptographic properties of these two keys and related cryptographic algorithms that use them are that their nature and functions are reverse to each other in the following sense:

(a) whatever the public key of one key pair encrypts, the corresponding private key decrypts, and reverse
(b) whatever the private key of one key pair encrypts, the corresponding public key decrypts

In public key cryptosystems the rule is that the pair of keys always belongs to one user. Bitcoin system uses asymmetric cryptographic algorithm called *Elliptic Curve Digital Signature Algorithm (ECDSA)*. With this algorithm each user, the member of the Bitcoin system, also has two keys. Public key is used as the element to derive the Bitcoin address that receives the payment. This cryptographic operation is called "digital enveloping". Private key is used to decrypt the balance of the wallet when making payments.

In the Bitcoin system, public key of a user's serves as the account address in user's wallet. Speaking precisely, during generation of the key pair and creation of Bitcoin addresses, the public key is cryptographically transformed into the Bitcoin address. The details of this transformation are not important. What is important is to remember that payment transaction to the Bitcoin account is created by encrypting the transaction using recipient's public key. Speaking precisely, the public key of an instance of the ECDSA algorithm that belongs to the recipient of a transaction is not used directly as an address of the receiving account. The Bitcoin account address is derived using public key as the parameter. This transformation is shown in Figure 3.

By the rules of public key cryptography outlined above, such cryptogram (in this case payment transaction) can be decrypted only by the corresponding private key, which is in the possession of the recipient of the transaction. This means, in principle and disregarding the details, that incoming transactions to some user's Bitcoin account

(a) are first encrypted by the sender using recipient's public key
(b) send to the sender in such encrypted form
(c) received and stored in sender's wallet in such encrypted form, and
(d) the corresponding private key is used before each outgoing payment to decrypt the received transaction, consolidate private ledger, create the updated balance of the sender's account and make outgoing payment.

The most important element for protection of bitcoins stored in the wallet, for opening the wallet and for making outgoing payments, is the private key. In other words, possession of the private key effectively means the ownership of bitcoins in the wallet.

This approach is the main reason why private keys are the most popular target of illegal attacks and thefts of bitcoins stored in wallets of individual users.

2.2 Distribution of Bitcoin Addresses – Step (2)

After completion of all communications that precede a payment transaction, such as establishing mutual communication link, negotiating purchase and transfer details, eventually exchanging and validating attributes and parameters characterizing each party, the last step in that pre-transaction exchange is for the recipient to pass the address of its Bitcoin account to the sender. As shown in section 4.1, that address is a long, humanly incomprehensible string of characters, so the address must be transferred either in a graphical form or as a message over-the-air.

If the two parties are in the proximity of each other and if both use some type of mobile device (smart phone or tablet), the address may be displayed by the recipient and picked up by the sender in the form of QR graphical image. If the sender is accessing Web server (of the merchant), the merchant may display the address of his/her Bitcoin account on its web page in the QR graphical form. If the two parties are remote, the recipient must transfer its Bitcoin address using some remote communication protocol (E-mail, etc.).

It is important to emphasize that the receipt of the correct and legitimate receiving Bitcoin account address is crucial for the payment transaction. Since the address represents public cryptographic key, if it is structurally incorrect (some bits modified during transfer), the amount of bitcoins in the transaction will be lost. Namely, in case of incorrect private key the transaction would be encrypted with the public key that does not have the corresponding private key, so the transaction is irrecoverable. The transaction would end up in a "black hole".

Standard concept and design of the Bitcoin does not have the solution for this problem.

Another reason why the Bitcoin address that the sender uses may be incorrect is due to the potential man-in-the-middle attack. If an intruder is listening to the pre–transaction exchange between two legitimate parties and then, inserts his/her own Bitcoin address instead of the address of the legitimate recipient, the sender would send bitcoins to an incorrect address. In this case, the payment also cannot be recovered by the recipient.

Current Bitcoin concept does not have the solution for this problem.

The conclusions of this discussion are that (a) it is absolutely important that the sender of the payment transaction receives correct and legitimate address for the payment, (b) if the address is structurally incorrect or does not belong to the correct partner, bitcoins transferred by the transaction will be lost, and (c) standard concept of the Bitcoin system does not have solution to this problem.

2.3 Opening Wallet and making Payment – Step (3)

After receiving the correct Bitcoin address for the payment, the sender uses his/her private key to open local wallet and make payment. Using the private key, all transactions stored in the wallet encrypted with the corresponding public key are decrypted, so that the amounts of bitcoins and the total balance of the wallet are now accessible.

The logic of the software or hardware wallet will check whether the balance in the wallet is sufficient to make the payment. If so, the wallet will create an outgoing transaction. After its creation, the transaction will be encrypted using the public key of the recipient, i.e. the address of the receiving Bitcoin account of the recipient, received in the previous step.

2.4 Opening Wallet and making Payment – Step (4)

Such encrypted transaction is not sent directly to the recipient. This shows that Bitcoin system does not perform peer-to-peer transactions. The transaction is in fact sent to the Bitcoin network.

Bitcoin network is a special network, comprising many communication and control nodes. They are all mutually linked through the special communication protocol that performs broadcast of the received transaction by the server that received the transaction to all other servers in the network. In addition to being distributed, global and synchronized, the Bitcoin network performs also several additional functions, all collectively called management and control of the Bitcoin system.

2.5 Packaging Transactions into Blocks – Step (5)

The Bitcoin network, more precisely its nodes,

(a) collect individual transactions for the time period of approximately 10 minutes,

(b) at the end of each ten minutes period, package them into specially structured block of transactions,
(c) based on the timing of the return of several previous blocks adjust the value of the target parameter and include it in the newly created block, and
(d) send such packaged block to special servers associated with the Bitcoin network, called Mining Servers.

These functions of the Bitcoin network clearly show that

(a) Bitcoin system is not peer-to–peer system, as claimed, because it uses third parties, i.e. the servers comprising Bitcoin network ([Franco, 2014], [Muftic, 2015]), and
(b) users have no possibility to test correctness of Bitcoin network operations, i.e. functions (a) to (d) above and they have to trust that the network will perform its functions correctly.

This shows that, contrary to the claims of the Bitcoin system, it uses many third parties and requires trust of users in operations of these third parties.

2.6 Validation of Blocks by Miners – Step (6)

Mining servers distribute blocks prepared by the Bitcoin network to their clients with special software modules, called miners. The analogy is with gold miners from the US history. Current block, being replicated to many Bitcoin network servers is distributed to many miners. They are all associated (connected) with their corresponding mining servers.

After receiving the current block, all miners iteratively perform the following cryptographic procedure with the block: in one iteration they generate random number, add it to the block, and calculate the hash of such block. Hashing is a simple randomizing function, so the produced hash is a random sequence of bits. Such hashes are acceptable in other security services (data integrity, digital signature, etc.), but not in the Bitcoin protocol.

In order to be accepted, the produced hash must have very special form: certain number of its leading bit positions must be equal to zero. This makes this type of hashing extremely difficult. The number of the required leading bit positions to be zero is determined by the Bitcoin network and the goal is to select hashing difficulty so that the new valid hash (block) is produced on average every ten minutes. In that way, the Bitcoin network takes into account the advances in chip technologies used for mining, with the goal of not creating new validated block to often, but on average each ten minutes.

Thus the process of collecting new transactions by the Bitcoin network and mining / validation of the current block are synchronized – each takes about ten minutes.

It is easy to understand why creating hash of the current block with certain number of leading zeros is so difficult. If the target has only one leading zero, i.e. hashes that have one leading zero are acceptable, then the probability of creating such hash is 50%, i.e. on average one in two hashes. If the target has two leading zeros, then the probability to create hash with two leading zeros is only 25% or one in four hashes. And so on. At the current level of difficulty targets have about 20 leading zeros, so the probability to create such hash is very low.

By the rules of the underlying cryptography for producing hashes it is not possible to adjust the value of the random number in the block with the goal to increase chances to create hash with leading zeros. The process is completely random, so the only approach the miners can

use is repetitive trial-and-error until the desired form of the hash is created by pure random outcome.

2.7 Return of Validated Blocks to the Bitcoin Network – Step (7)

When some miner succeeds in creating correct hash for the current block, he/she returns such new block to the Mining Server and the server returns it to the Bitcoin network.

The network, first, rewards the miner who created new block with the reward paid in bitcoins. The reward varies by time and it changes every four years. It started at 50 bitcoins for the period 2009 – 2012. At the moment it is 25 bitcoins (2013 – 2016). The next four years it will be 12.5 bitcoins. The miner who receives the reward stores it in his/her wallet and can use it for payments or put it for sale (cash-out) to one of the auction servers.

Miners usually work in teams ("pools") so that when one member of the pool creates the target hash, all members share the reward.

In addition to payout of the reward, Bitcoin network performs also the following two actions:

(a) The node that received the new block distributes it (broadcast) to all other nodes in the network, and
(b) The network adjusts the target if necessary, i.e. it increases the number of leading zeros in it, if several of the most recent replies arrived on average in time periods shorter that 10 minutes.

2.8 Distribution of the New Block to all Users – Step (8)

When each node in the Bitcoin network receives new validated block, it distributes it to all Bitcoin wallets of users linked to that network node. In fact, for redundancy and availability, each wallet is linked to several of the Bitcoin network nodes.

With this download, each wallet receives all new transactions performed in the global Bitcoin system in the last ten minutes. One of these transactions is presumably the transaction by the sender, created in the step (3). Since individual blocks are hashed by the very complicated and computing intensive procedure, all users are convinced that the content of the block is correct, as it is impossible to tamper with it. The blocks also cannot be illegally inserted in the blockchain, since they are mutually linked ("chained") by the hash of the previous block inserted in the current block.

Upon receiving the latest validated block, the recipient still cannot consider the transaction created in step (3) as confirmed. There are two reasons for that.

The transaction is presumably included in the newest block, but that may not be the case [Bitcoin, 2010]. The reason why specific transaction may not be in the newest block is that it was late for inclusion in the block, due to delay in its propagation through the Bitcoin network. If that is the case, the transaction will be, most probably, included in the next block, so in that case the recipient must wait for the next validated block. The transaction will be included in the block if miners are honest and process all transactions that are included in the block. But, in case of dishonest miners, they may eliminate some transactions from the block.

Bitcoin concept and current operational version has no remedy for this problem [Ali, 2016].

The other reason is that the transaction may be included in two or more validated blocks. Such situation is possible because validation procedure (hashing) of the current block is performed in parallel by many miners. Therefore, there may be the situation where two or

more miners simultaneously create valid hash. Each of them will include it in the block and the block will be appended to the latest version of the blockchain. But, since appending is performed by multiple Mining Servers, in this case the blockchain will have several branches - forks. Therefore, all users, among them the recipient of the transaction created in step (3), will receive several different copies of the blockchain.

To resolve this situation and return the blockchain to the single thread version, the rules for appending new validated blocks by the Bitcoin network are the following:

(a) Each node will append the new block to the longest blockchain branch, the one that has the largest number of newly appended blocks in the branch.
(b) If all branches contain the same number of blocks in the branch, then the new block will be appended to the branch whose latest block has the earliest creation date.

With these two rules, after several new validated blocks are appended to one of the blockchain branches, one of these branches will start to ”dominate” the blockchain. That branch will become the main branch of the blockchain and other branches will “die out”, i.e. they will not be used and the copies of all their transactions will be contain in the dominant branch.

Therefore, after receiving the latest block, the recipient cannot assume that the transaction is validated, as it may be included in the branch of the blockchain that will be discarded. If so, the valid copy of the transaction will finally be in the main blockchain branch. The empirical rule for this convergence of several blockchain branches into the main branch is to wait for six blocks to be added to the blockchain. Time wise, that is approximately one hour.

This situation – branches of the blockchain and their elimination using the procedure of delayed validation for about one hour, makes Bitcoin protocol very inconvenient for many types of payment and financial transactions. It is inconvenient to make payments over-the-counter. The system is not convenient to support time-sensitive financial transactions, like trading stock, paying for auctions, lotteries, etc.

This inconvenience cannot be resolved by simple modification of the Bitcoin protocol, as it is inherently built into many components and aspects of the system and reflects it operational design and philosophy.

Support for time-sensitive transactions require design of the new system that, as one of its properties, will provide instantaneous validation of transactions.

3 Additional Components and Extended Architecture

3.1 Additional Functions and Services

Bitcoin is the payment system where logical relationship between two transaction parties is peer-to-peer. It has inspired many additional ideas, concepts and developments. The general approach in all these new initiatives is the suggestion to use direct peer-to-peer relationship between two transaction parties, without any third party. As explained in section 1.3 such transactions are very efficient, but providing their validation, security, and privacy, without participation of any third party, is very difficult.

Bitcoin system solved that issue by using special, cryptographically protected form of the transactions archive – public ledger (blockchain) and special transaction validation protocol. New ideas and initiatives are all based on the same principles introduced by Bitcoin. They all can be classified in four global categories:

(a) Establishment and operations of payment systems equivalent to the Bitcoin, but based on alternative crypto currencies.
(b) Establishment and operations of payment systems that do not use crypto currencies, but some alternative form of virtual currencies.
(c) Establishment and operations of various additional system components that provide services for payments using either Bitcoin or any other virtual currency, which are necessary or convenient for the Bitcoin payment transactions.
(d) Design, development and deployment of alternative systems that manage and use general types of digital assets, not only financial assets (crypto currencies or virtual currencies), but assets such as intellectual property, real estate, jewelry and valuables, electric energy, valuable documents, etc.

This chapter describes those additional components of the Bitcoin system that provide additional services in the categories (a), (b), and (c). Different types of such components are shown in Figure 2 and brief description of services provided by each of them is given in the rest of this chapter:

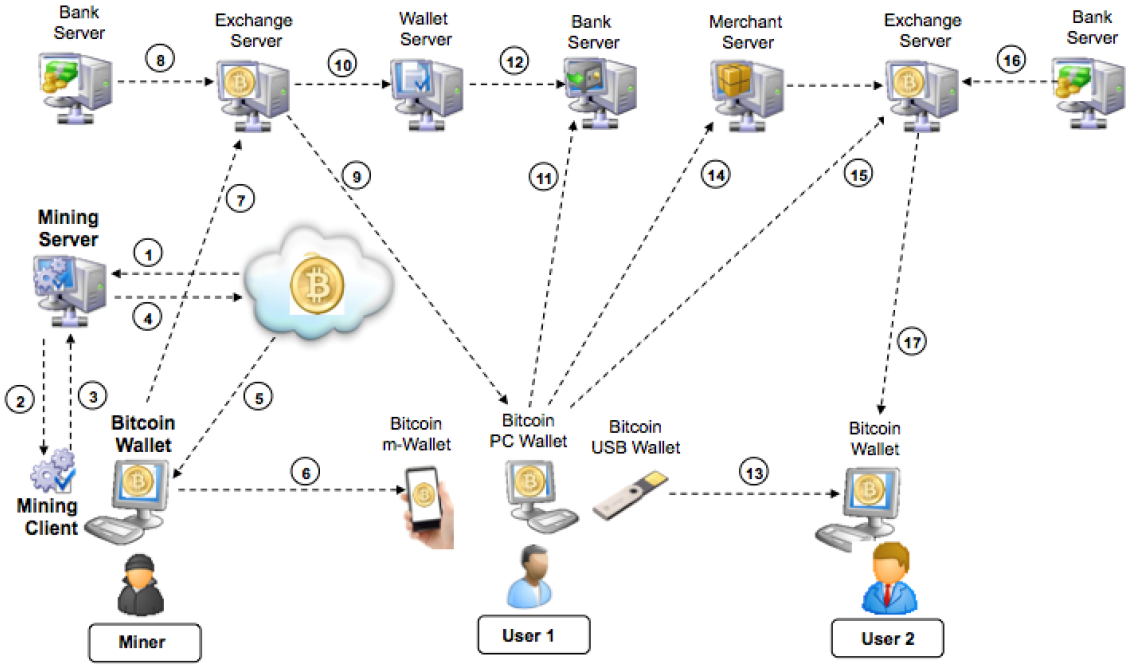


Figure 2. Additional Components and Services

3.2 Bank Server

Bank Server is a special interface between standard financial institutions and the system handling various types of virtual currencies. Its function is to convert real-world currencies into their digital equivalents – virtual currencies. The conversion may be into prepaid cards, gift cards, air-time and other form of digital financial assets.

The virtual currencies created by conversion of real-world currencies are not bitcoins. They do not use Bitcoin protocol for validation of transactions. Transactions are validated using transaction chains, each element represented by a pair of virtual accounts and accounts organized in the chain by the respective payment transactions.

The transaction by which the owner of the real-world account in the financial institution that uses this Server converts real-world currency into an equivalent amount of virtual currency is the initial, trusted transaction. It represents the head of the transactions chain for the specific amount of virtual currency.

This server may be used with two purposes. One is to link to the Exchange Server, so that customers with real-world bank accounts may use real-world currencies to buy virtual currencies. The other purpose of this server is to be a "connector" for bank-to-bank account transfers using blockchain technology. It has been already mentioned that the current inter-banking network is very complex and expensive. Blockchain may be an alternative, more secure, and simpler infrastructure.

If such infrastructure is used, then bank-to-bank account transfers from the originating to the receiving account are performed through the connectors that link standard bank servers to the virtual currencies network. Multiple such connectors may be used. One is associated with each bank, so that transfer is performed as multiple "hops" between multiple Bank Servers [Thomas, 2016].

3.3 Exchange Server

The main functions of the Exchange Server are to support selling and buying Bitcoins through auctions or as sale with fixed price. The members of the Bitcoin system may upload their bitcoins and offer them for sale by declaring either fixed price or minimum acceptable auction bid price.

Bitcoins offered for sale are usually uploaded into an escrow Bitcoin account, owned by the Exchange Server operator. Upon completion of a sale or auction and after collecting payment for bitcoins in real-world currency from the buyer, the Exchange Server transfers bitcoins to the Bitcoin account of the buyer.

With the current version of the Bitcoin system, this transaction has several serious problems. First, many exchanges have been hacked and all bitcoins stored in their escrow accounts have been stolen. Second, the members participating in the auction must trust the exchange to transfer the Bitcoins after they purchase them and pay in real-world currency. Also, most of the exchanges, before transferring real–world currency into bitcoins require full and explicit identification of buyers what violates the basic principle of anonymity of Bitcoin users.

Current concept and operational version of the Bitcoin system does not have a good solution for these problems.

3.4 Online Wallet

Online Wallet is usually web server where the members of the Bitcoin system may deposit their bitcoins. The reason for depositing bitcoins may be that some members of the Bitcoin system do not have IT devices with storage capabilities (PCs or smart phones). The other reason is to use Online Wallet as safe storage of bitcoins.

These online Wallets usually also provide the possibility to perform transactions with stored bitcoins. Therefore, they are usually called "*hot wallets*". User access those wallets using their browsers or remote mobile applications. The main feature of these wallets is that they store the complete user's wallet, including his/her private keys that are needed in order to use the wallet and manipulate with bitcoin currency stored in it. Therefore, identification and authentication of users, before accessing and using their online wallets and also strong protection of users' private keys, are important prerequisites and requirements for correct functioning of these wallets.

Online wallets are also vulnerable to the same type of problems as Exchange Servers.

3.5 Merchant Server

Merchant Servers are usually Web servers that in the background run Bitcoin Wallet. With such servers, merchants can display their Bitcoin account addresses in the form of QR code, that enables easy access and payments by other members of the Bitcoin system.

Upon accepting payment initiation transactions, usually from users' browsers or mobile phones, the background modules of the Server perform payment transactions with bitcoins. In this case, the server is the recipient of the transaction. So, when a visiting consumer performs the transaction using his/her wallet, merchant's server displays the transaction as the receiving transaction.

3.6 Flow of Bitcoins and Virtual Currencies

The flow of bitcoins and other virtual currencies between individual components of the extended architecture for the Bitcoin system is shown in Figure 2.

For new bitcoins the flow starts with the Bitcoin network collecting all current payment transactions into a block and sending them to all Mining Servers – step (1). Mining servers send them to mining clients – step (2). After validation and creation of the new block, the block is returned to the Mining Server – step (3). Mining Server that received new block, returns it to the Bitcoin network – step (4).

Upon receiving new block, Bitcoin network generates the reward as new bitcoins and sends them to the miner that generated new validated block – step (5). That miner may share the reward if he/she was operating as the member of the mining pool.

The miner(s) who received new bitcoins may use them to pay to other members of the Bitcoin system – step (6) or offer them for sale by depositing them to the Exchange Server – step (7).

Other virtual currencies may be generated by converting real-world currencies into the equivalent virtual currencies – step (8).

When bitcoins are purchased at the Exchange Server or new virtual currency has been generated, Bitcoin system member may transfer the currency either into a local Wallet – step (9) or into a Wallet Server – step (10).

If bitcoins or other virtual currencies are not needed any longer, bitcoins may be offered for sale at the Exchange Server – step (15) or virtual currency may be converted back into real-world currency from the local wallet – step (11) or from the Wallet Server – step (12). During the purchase of bitcoins, a transfer of real-world currency may be needed – step (16). The new owner receives bitcoins to his/her wallet – step (17)

To receive on-line payments merchant may use web servers to display their Bitcoin account addresses. Bitcoins are transferred as payments form local wallet (or Wallet server) to the wallet of the merchant, operating in conjunction with the merchant's front-end store web server – step (14).

4 Anonymity of Users and Transactions

4.1 Generation of Bitcoin Addresses

It was already mentioned in section 3.1 that Bitcoin address of an account in fact represents the public key of the public key cryptographic algorithm. Precisely, the address is not the public key itself, but a random string generated by the especial cryptographic procedure based on the public key as an input parameter. The most important is that the payment transaction, which is encrypted with such address, can be decrypted using the private key that corresponds to the public key used to generate Bitcoin address.

The procedure to generate key pair in the Bitcoin system is shown in Figure 3.

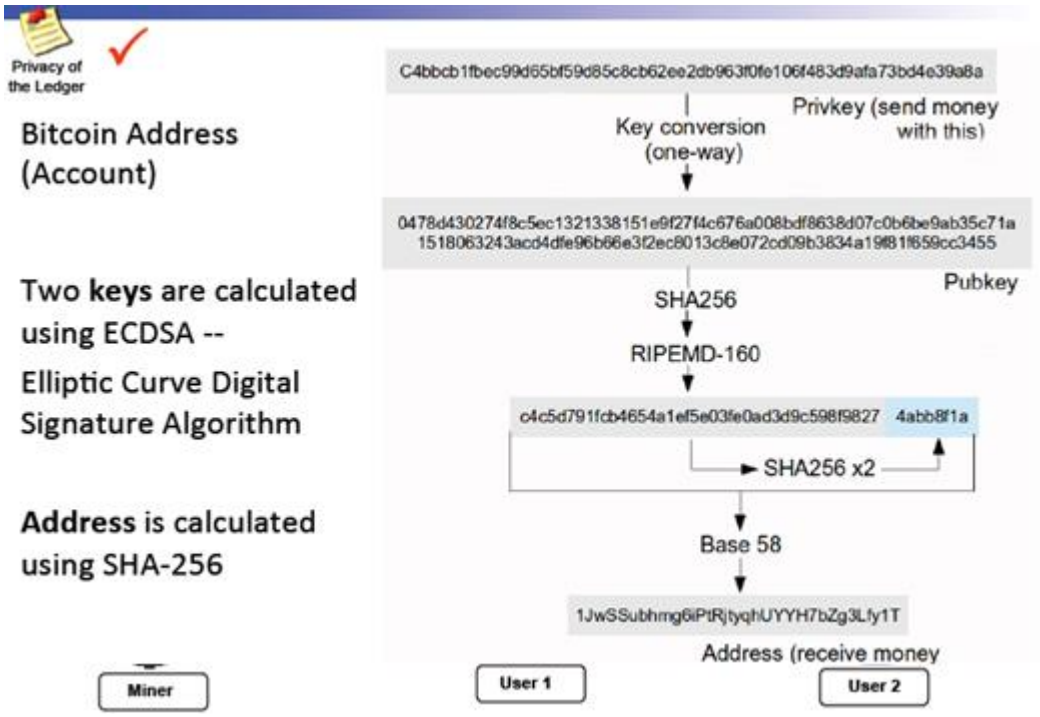


Figure 3. Generation of Bitcoin Keys and Addresses

Bitcoin uses specific asymmetric cryptographic algorithm called Elliptic Curve Digital Signature Algorithm (ECDSA). Special feature of this algorithm, compared with other types of asymmetric cryptographic algorithms, is that the private key in an instance of the pair of keys is a random number. This property makes it easy to generate. Using private key as the parameter of the key generation procedure, the corresponding public key is generated.

Then, in the Bitcoin system, that public key is converted into the Bitcoin account address by the sequence of special cryptographic steps. Bitcoin address is distributed to transaction partners who use it to encrypt transaction when making payments. Private key is used by the recipients of transactions to decrypt (open) the transaction and use bitcoins in it to make further payments.

4.2 Anonymity of Users and Transactions

Use of public keys as Bitcoin addresses has several advantages:

(a) They can be publicly distributed to all system participants, so that any member of the Bitcoin system can make the payment to the address / account owner.
(b) Using addresses as public keys for cryptographic transformations of payment transactions makes them protected against any other (legal or illegal) user in the system, as only the correct recipient, who owns the corresponding private key, may receive the transaction and further use bitcoins in it.
(c) Since addresses are not linked to any type of identities of users, they provide anonymity of users and their transactions.

Interpreting this approach and protocol in terms of standard security services, it is clear that Bitcoin system provides transaction's data confidentiality, data integrity, recipient's authenticity, and recipient's anonymity.

These are the four main security services needed in any payment system as they, in a broader interpretation, reflect the rules of "perfect" payment transaction – using cash over-the-counter.

4.3 Negative Implications and Consequences

Direct use of cryptographic keys to make / protect payment transactions by their senders and to receive / use bitcoins by their recipients, in addition to all the benefits mentioned in the previous section, has at the same time some serious negative consequences.

The first one, already mentioned, is that it requires very precise, accurate and guaranteed *distribution* of Bitcoin account addresses. If the address is in any way modified in transfer, the user will make irrecoverable payment. If the address of the legal recipient is illegally substituted by an address of an illegal user, the payment will be made to an illegal user.

The next disadvantage of the current Bitcoin system is the possibility to perform transactions that are illegal or against financial regulations. Examples of such transactions are laundering money, issuing ransoms, avoiding taxes, etc. The "enabling" feature for such transactions is the anonymity of Bitcoin addresses and users. The anonymity is a desirable property between transaction partners and against other users in the system. But, it Is not desirable in case of illegal and transactions that are against financial regulations.

Another disadvantage based on the rules of public key cryptography is that transactions are *irreversible*. This property is not always desirable in real-life payment situations, as there may be cases when a payment needs to be cancelled or otherwise returned to the sender, without making reverse payment by the receiver.

The most serious problem is *loss* or *theft of a private key* that opens the wallet of the user. If the user loses his/her private key all Bitcoins stored in the wallet are irreversibly lost. Even worse, if the private key is stolen, the Bitcoins in the wallet will also be stolen.

The general principle of using public key cryptography for security services of Bitcoin transactions is obviously a natural approach. But the specific principle of using public and private keys to directly enable payment transactions is not a good principle. Damage of the public key and theft/loss of the private key create irreparable consequences, not only to the owner of the specific wallet, but also to the entire community.

However, using key pairs as parameters to provide security services for any application's transactions, elements and attributes, requires a sophisticated system for management of these keys. It is well known that the best current solution for management of private keys is the use of *smart cards*. But, this solution is not suitable for large-scale deployment and use of the

Bitcoin system. The current solution for management of public keys is to use Public Key Infrastructure (PKI). But, that solution requires the use of third parties with the full trust, what is contradictory to the core principles of the Bitcoin system – (a) supporting direct peer-to-peer transactions between the partners, (b) without participation or support of any third party, and (c) without the need to place trust in any component of the system.

Solutions for these and all other problems and for their negative consequences cannot be established by minor improvements and adjustments of the current Bitcoin system. New and innovative ideas, concepts, and solutions are needed to solve these problems and thus to effectively enable secure, private, anonymous, and reliable transactions.

5 Conceptual Issues for Peer-to-Peer Financial Transactions

5.1 Validity of Users and Transactions

Bitcoin payment transactions establish peer-to-peer logical relationship between transaction parties. The system is based completely on digital resources, software modules, and protocols. It operates in a completely open environment and supports transactions between community of system members. Those members are anonymous and for each transaction the parties are mutually unknown to each other, mutually unrelated, and usually mutually suspicious.

Regardless of all these circumstances and arrangements, the transactions in the system must be validated by each party – usually the recipient. Validation comprises verification that (a) the sender is regular user in the system, that (b) the currency he/she uses is correct crypto currency, and that (c) the sender has sufficient amount of currency in his/her wallet when performing payment transaction.

All these aspects and issues that recipients of transactions are facing must be validated within the environment without assistance of third parties and without the requirement to place trust in any party in the system. The concept of the Bitcoin claims to have solved these important problems for payment transactions, but also for any other type of a serious and sensitive peer-to–peer transaction.

When a payment transaction is initiated / performed between the two parties, the receiving party is concerned with several issues and problems that must be solved in order to accept the payment as a valid transaction. Some of those issues, addressed and solved by the concept of Bitcoin, are described in this chapter.

However, there are a number of additional problems and issues in the Bitcoin system that are not addressed by the concept of the Bitcoin. Quite contrary, some of these issues are in fact caused by an inadequate concept of the Bitcoin system. These problems and some potential solutions for them are described in Chapter 6.

5.2 Proof of Possession

When the recipient receives the payment, his/her first concern is whether the sender possessed sufficient balance of Bitcoins in his/her wallet to make the payment. Since the system is completely digital, the issue for the recipient is whether the sender made the payment using legitimate currency or the transaction was “fabricated” without sufficient amount of Bitcoins in the sender’s wallet.

The first criteria / test for this issue is the question whether the sender received the amount of Bitcoins equal or greater to the amount in the current payment transaction in a transaction from some other sender before the time of the current transaction. The logic of this test is that, if the sender has received an amount equal to or greater than the payment amount in the current transaction, then he/she is in a possession of sufficient amount of Bitcoins to make the current payment.

5.3 Prevention of Double Spending

The test in section 5.2 – proof of possession, is effective provided that the sender did not double spend the received amount. The logic of this test is the following: if the sender indeed

earlier received an amount of bitcoins equal or greater than the payment amount in the current transaction and did not already use these bitcoins to pay to some other user, then the conclusion by the recipient is that the sender still has sufficient amount of bitcoins in his/her wallet to make current payment.

Double spending is a legitimate concern in the Bitcoin system and in other similar systems, because:

(a) the system is completely digital and therefore, in principle, even after sending certain amount of bitcoins to some recipient, the sender may still be in a possession of the same bitcoins, due to their digital nature, and
(b) the system does not use the services of third parties to maintain the balance of sender's account after making the payment.

The conclusion is that the current transaction is valid if the sender has not made another, previous transaction, using the same amount of bitcoins received from some previous sender.

5.4 Validity of a Transaction based on Previous Transactions

Based on the two tests outlined in section 5.2 and 5.3, the conclusion by the recipient is that the current payment transaction is valid provided that

(a) the sender can show that he/she has received the same or greater amount of bitcoins as in the current payment transaction from some other user at the time that is earlier than the current transaction, and
(b) the sender can show that he/she did not spend previously received amount of bitcoins as payments to some other recipient with the transaction at the time earlier than the current transaction

These two conditions / tests effectively mean that the recipient wants to be absolutely certain that the sender has in his/her possession a sufficient amount of bitcoins to make the current payment. Violation of any of the conditions (a) or (b) would effectively mean that the sender is "printing money". If such action would be possible that would completely destroy the trust in and therefore reliability of the entire system.

5.5 Validity of a Transaction based on a Personal Ledger

The two conditions described in section 5.4 are satisfactory to make the current payment transaction valid. But, they are not mandatory. The reason is that there may be a situation where these two conditions have not been met, but the current transaction is still valid. More specific, the sender of the current transaction may not have previously received a payment with the amount equal or greater of the current amount or that even the sender has made previous transaction equal or greater than the current payment amount, but the current payment transaction is still valid.

Namely, the essence of the validity of the current payment transaction is the condition that the sender has sufficient amount of bitcoins in his/her account to make the current payment. The sender, indeed, may have such amount without conditions (a) and (b) being satisfied. The balance of the sender's wallet is created by crediting it with amounts of all bitcoin transaction that the sender has received (so called *incoming transactions*) reduced by the amount of payment transactions that the sender has made (so called *outgoing transactions*).

Each participant in the system keeps the log of all his/her incoming and also outgoing transactions. That log is called the *ledger* and since it is maintained by each person, it is called *personal ledger*. The entries in the ledger are all incoming and all outgoing transactions that the person has performed and as the result of each transaction an updated balance is maintained. Therefore, personal ledger contains all previously performed transactions and clearly indicates the balance of the wallet of each person participating in the system.

As the conclusion and as the requirement that extends conditions (a) and (b) in section 5.4, in order to verify the validity of the current payment transaction, the receiver would like to verify the balance of the sender's personal ledger. So, instead of asking the sender to prove conditions (a) and (b) from section 5.4, the recipient in fact requires from the sender to send his/her personal ledger together with the current payment transaction. Inspection of the ledger for correctness of all its entries and therefore the current balance of the sender's ledger at the time of the payment transaction represents validation of the correctness and validity of the current transaction.

5.6 Sharing of Personal Ledgers

Therefore, in order to enable the recipient to verify the correctness of the current payment transaction, the sender sends to the recipient his/her personal ledger together with the payment transaction. But, this transfer, although seems logical and necessary, as explained in section 5.5 above, has several problems.

The first problem is for the sender, as he/she must share all his/her previous transactions with the recipient of the current transaction. This action violates sender's privacy and anonymity. Therefore, in order the Bitcoin system to be acceptable to its users, this problem must be solved. The contradictory requirements in fact are that

(a) the recipient must have at his/her disposal the full personal transactions ledger of the sender that includes all his/her previous transactions, while at the same time
(b) the sender requires personal privacy and anonymity so that transactions in the personal ledger cannot be linked to and traced back to the specific sender.

The solution for these two contradictory requirements will be described in Chapter 6.

5.7 Integrity of Personal Ledgers

Even if the sender sends his/her personal ledger to the recipient for validation of the current transaction, as described in section 5.5, the validation of the transaction still cannot be correctly performed. There are two reasons for that, one is explained in this section, another is explained in the next section.

The first reason why the recipient cannot use personal ledger of the sender to validate correctly the transaction is that the ledger can be manipulated by the sender. Namely, the sender can, before sending the ledger to the recipient, either

(a) add into the ledger one or more incoming transactions and in that way increase the balance of the ledger, or
(b) remove from the ledger one or more outgoing transactions and in that way, also, increase the balance of the ledger.

The conclusion is that, in order to eliminate these potential modifications of the personal ledger, the ledger must be protected against such illegal modifications – deletions and insertions. In other words, security service called data integrity must be applied to the ledger. It is well known that data integrity is provided by the cryptographic mechanism called hashing. In that process, digital digest (hash) is created using the content of the entire ledger and appended to the ledger. Then, the content of the ledger may be validated by the recipient by creating the hash of the ledger and comparing it with the hash created by and received from the sender.

However, even this step is not sufficient to guarantee the correctness of the personal ledger. The reason is that the sender can create the described hash after illegally manipulating the ledger. Therefore, in order to make this security service applied to the personal ledger effective, the conclusion is that

(a) the personal ledger must be hashed in order to provide to the recipient the possibility to validate its correct content, but
(b) hashing cannot be performed by the sender, as this approach opens the possibility of illegally manipulating the ledger before creating and appending the hash to it.

The solution to this requirement for the hashing procedure is explained in section 2.6.

5.8 Personal Ledgers of Previous Senders

The other reason why the recipient cannot use personal ledger of the sender to validate current transaction is that it includes many incoming transactions. These transactions were sent to the current sender by other users in the system. However, each of these transactions is unreliable to the recipient of the current payment, as they all must be validated for the same prerequisites stated in section 5.4 that were applied to the current payment transaction. Namely, for each incoming transaction of the current sender, the recipient must be able to validate those transactions, but now with respect to the two prerequisite issues applied to all the senders of all incoming transactions in the personal ledger of the current sender.

Applying the same logic and the same approach described in section 5.4 to the personal ledger of the current sender, the conclusion is that the recipient of the current payment transaction needs personal ledgers of all users in the system that sent payment transactions to the current sender. These senders may be called “previous generation” of senders. At the moment, the only way for the recipient of the current payment transaction to get these personal ledgers is to receive them from the current sender, who has received them in the process of verifying his/her incoming transactions.

5.9 Bitcoin System Global Ledger

The logic and the approach with personal ledgers of the previous senders of incoming transactions for the current sender applies recursively to their previous senders, i.e. to senders belonging to the “two generations” backwards with respect to the current sender. But, this process does not stop there, as equivalently, personal ledgers of yet another previous generation of senders are also needed.

This reasoning and the approach leads to the conclusion that, since any member of the Bitcoin system may in one of all previous transactions be the sender of bitcoins that finally reached the recipient in the current payment transaction, the recipient needs personal ledgers of all users in the system. In other words, the recipient needs the complete global transactions

ledger of the entire system. This ledger contains all transactions that were ever performed in the system.

This conclusion leads to the following two problems:

(a) How is the complete system-wide ledger distributed to each participant in the system, and
(b) Which user is the sender of the first, initial outgoing transaction for the certain amount of bitcoins, since the dependency of each sender on some previous senders must originate at some point.

The conclusion that there must be some user(s) in the Bitcoin system that are senders of bitcoin payment transactions, but without having previous senders, leads to the conclusion that some users in the system are in possession of bitcoins without having received them from any other users.

The questions who are these users and how they have in their possession certain amount of bitcoins without receiving them from any other user will be answered in the next chapter of this Report.

6 Weaknesses, Vulnerabilities, Threats and Problems

6.1 Approach

This chapter describes weaknesses, vulnerabilities, threats and problems with the Bitcoin system. Weaknesses are deficiencies of the concept that may cause inconveniences for the use of the Bitcoin system or inadequacies for some additional applications. Vulnerabilities are both conceptual and also implementation issues that may cause problems if triggered by unintentional incorrect operations. Threats are serious issues that can be explored by illegal users as intruders or as man-in-the-middle activities. Finally, problems are situations and issues that cause serious harm to regular users, resulting in their loss of bitcoins.

All the issues with the current Bitcoin system are structured in four categories:

(a) Problems caused by users and problems for users
(b) Problems caused by miners
(c) Problems with exchanges caused by hackers
(d) Problems caused by man-in-the-middle attacks

Bitcoin is becoming very popular, efficient and convenient way of making person-to-person payments and the total value of Bitcoins in the network is continuously increasing. So is the number of transactions. Besides its attractiveness to perform legal transactions and to be used by regular users, this trend, combined with various Bitcoin system vulnerabilities, is unfortunately also increasing the number of illegal and destructive activities.

Bitcoin transactions and resources are becoming a target of many standard security penetrations and attacks, as well as some attacks that are based on specific rules and weaknesses of Bitcoin system operations. Unfortunately, no comprehensive solution has been proposed so far for these problems. Therefore, sometimes there is an impression in general public that Bitcoin has more negative aspects than positive features and benefits.

Most issues and weaknesses of the current Bitcoin system cannot be eliminated by small, standard security patches and "tweaked" security services. This fact implies the need of certain modifications of the concept as well as the Bitcoin protocol. The difficulty of this approach is that (a) all the currently suggested modifications are not backward compatible with the current version of the system, and (b) they must be adopted and deployed by the consent of the entire Bitcoin community. This means that modifications and improvements are all-or-nothing approach, which is always problematic for adoption and deployment.

As described in detail in Chapter 3, the flow of data for a payment transaction starts at a sender who has installed Bitcoin wallet on his/her workstation or mobile device in order to send some bitcoins to the receiver. The sender's Bitcoin wallet is prone to many problems: first its software is vulnerable to malware attacks and, second, encryption of its local secret parameter (private key) is weak and vulnerable to the theft. Both of these cases can result in a theft of private keys used by the wallet and in that way the complete loss of bitcoins stored in the wallet.

In addition, since the system is fully digital and there are no accompanying documents, the transaction sender can trick the receiver by double spending the amount of bitcoins he/she has paid to the receiver. Hence, the sender can deprive the receiver from the sent bitcoins and can reuse those bitcoins. Users may also try to fabricate illegally new amount of bitcoins, simulating the operations of the network. In the Bitcoin system the components of the

network cannot be authenticated and the correctness of its operations cannot be validated. Therefore, in addition to denial-of-service attacks, the hackers or even regular users may attempt to simulate the operations of the network. One of the critical functions is generating new amount of bitcoins.

There are problems with miners and their operations too. Malicious mining is a major threat for Bitcoin transactions. If malicious miners achieve a very high hash rate, they can easily add illegal transactions into the Bitcoin blockchain and in that way they can steal bitcoins from regular users. This threat can be achieved without any illegal operations in the system, but just by using advanced IT devices or by pooling a large number of miners into a single mining pool.

Finally, Bitcoin transactions which were initially claimed to be completely anonymous can reveal the identity of the transaction parties [Reid, 2012]. One source of such information are identities of Bitcoin users revealed by users themselves. Namely, in order to buy bitcoins from exchanges, Bitcoin users have to provide their clear identifying personal information. Using this information in order to purchase an initial amount of bitcoins, can be used to trace further all outgoing transactions from the account receiving bitcoins from the exchange. In the process of buying bitcoins at the exchanges, the personal information can be a victim of man-in-the-middle attack. Additional problems with personal information and users' anonymity are malicious or hacked exchanges. In fact, weaknesses and hacking of exchanges is one of the most common problems with the current deployment of the Bitcoin system.

The following sections describe some attacks that are possible in the Bitcoin system.

6.2 Attacks by Regular Users – Double Spending

During execution of a single transaction, i.e. the time between the moment when the sender has submitted the transaction into the Bitcoin network (step (4) above) and the moment when the recipient has finally accepted the transaction as confirmed (step (8) above), there is a possibility for the sender to send the same bitcoins to two different receivers within the single transaction cycle time interval. This leads to a problem known as double spending [Karame, 2016]. One possible way to deal with this situation is to introduce a trusted third party or a mint that keeps a record of all transactions and continuously checks each transaction for double spending [Bitcoin, 2009]. However, this approach is contrary to the concept and principles of the Bitcoin system, since with that approach the system will be dependent on the services of the trusted third party [Drainville, 2012]. The best possible countermeasure for double spending in the current scenario is public announcements of all the transactions to all the members in the Bitcoin network, but not after ten minutes, but immediately in the moment when the transaction is initiated.

With this approach, the transactions in the blockchain ledger would be in three states: submitted, temporary approved, and finally approved. If this approach were to be introduced, it would obviously mean that the structure and processing of individual blocks must be changed, the structure of the blockchain ledger must be changed, and the Bitcoin protocol must be changed. The solution is very effective, but its implementation is very complicated for the current concept and implementation of the Bitcoin system. Therefore, obviously, some alternative and more efficient solution for this problem is needed.

Double spending attacks occur when a user sends the same amount of bitcoins to more than one user as one transaction immediately followed by the other or within the same transaction cycle time period. Bitcoin system uses specially created hashes based on proof-of-work schemes to protect against double spending attacks. But attackers have found ways to bypass

such schemes. One of the possibilities of double spending is that the attacker tricks the recipient by sending him/her a transaction which actually cannot be redeemed. In order to avoid detection, attacker has to replace the transaction as well as the block in the blockchain which has incorporated that transaction. This requires a lot of computational power due to re-computation of that block as well as all subsequent blocks in the block chain.

Double spending attacks are more serious in protocols with fast payment turnaround times where the time to exchange payment between the sender and the receiver is very short.

6.2.1 Attacks in the Case of Standard Payment Transactions

Whenever a payment transaction is initiated, the sender submits the transaction to the Bitcoin network and the node receiving the transaction broadcasts it to the entire Bitcoin network. Each Bitcoin network server verifies that the transaction is correctly structured and that the amount has not been previously spent by the same sender. This test is performed by verifying the balance of the sender's Bitcoin account before making the payment. The balance is verified using the current version of the transactions blockchain. After this verification, the transaction is packaged into the current block and at the end of the ten minutes' interval, the block is passed to the Mining Servers.

Each miner then competes in the mining process by trying to create the correct hash for the block. If a miner succeeds in finding a nonce that creates correct hash, it packages the new validated block. This block is then returned to the Mining Server that returns it to one of the Bitcoin network servers that broadcasts it to the entire Bitcoin network. After receiving such validated new block, each Bitcoin network server verifies that the block is valid and that every transaction incorporated in it is not double spent transaction. If verification is successful, the block is added to the blockchain.

However, in spite of this seemingly efficient cryptographic procedure, attackers were successful in performing double spending attacks. Some of the attacks in the presence of block confirmations are the following:

Brute Force Attack: The chances of a brute force attack being successful depend on the attacker's computing capabilities expressed as the hash rate. If an attacker has at his/her disposal advanced IT capabilities that create very high hash rate, then this attack can be successful with a high probability. In this case, the attacker makes a payment transaction to the recipient, but in the meantime keeps mining the conflicting block. If successful, the attacker creates a fork in the blockchain in which a double spending transaction is included. After receiving the bitcoins, the recipient waits for additional confirmations and then accepts the payment. Once the transaction in the fork is accepted, the attacker releases the fork included in the main blockchain for overtaking the number of blocks on the alternative fork of the blockchain. It is clear that such attack can be successful only if the attacker can overrun the creation of the alternative fork in the blockchain and in that way eliminate the fork in which one of his/her double spent transactions was included.

51% Attack: This attack also requires an attacker to have at his/her disposal IT equipment that can produce more than half of the networks hash rate. All of the bitcoin transactions are incorporated on blockchains. Whenever a new transaction takes place, it is added to a block which is then appended at the end of the blockchain. In the presence of some conflicting transactions, a fork occurs in the block chain and miners have to vote for the block they think is valid. Voting is done by appending further blocks to the block the miners think is valid. The longest block chain is accepted whereas the other one is discarded.

If the attacker controls majority of the networks hash rate, he/she can create blocks faster than the rest of the network. Attacker can intentionally create conflicting transactions and can get them verified by the network by generating blocks in order to keep the chain longer than that of the legitimate users. This attack can be successful not only for new, illegitimate transactions, but also for previously approved transactions.

It is very interesting to note that payment systems that use alternative virtual currencies, not bitcoins, are especially vulnerable to this attack. The reason is that all such schemes usually have very short blockchains which may be easily overrun by powerful miners.

6.2.2 Attacks in the Case of Fast Payment Transactions

If payment transaction does not contain high value, it is possible to process it under the accelerated procedure. The approach is to let the recipient use the received amount of Bitcoins without waiting for six validation blocks. In this type of payment transactions most of the times, the transaction is not of high value and the availability of bitcoins for the recipient is immediate. This means that transaction cycle is completed without the full validation cycle. For standard transactions, it takes on average of 10 minutes for a transaction to be validated and reliably included in the main branch of the blockchain. Certain recipients, such as fast food restaurants, supermarkets, ATM machines, vending machines etc. cannot wait too long for the transaction to be confirmed in order to provide their services.

Therefore, in order to accommodate situations with the requirement for faster payments Bitcoin system allows special type of processing, so called *zero confirmation* transactions. This means that the availability of the paid amount of bitcoins is immediate. Current version of the Bitcoin system does not have protection mechanism against double spending in case of fast processing payment transactions. An attacker can create two conflicting transactions where one of the transactions transfers bitcoins to some recipient, whereas the other sends the same amount of bitcoins to an account owned by the attacker.

The following two are important attacks related to double spending in the case of fast processing transactions:

Race Attacks: The degree of success of race attacks in the Bitcoin protocol is very high. There are examples how attackers can successfully double spend bitcoins in spite of the current version of the Bitcoin protocol that presumably prevents that to happen [Perry, 2012]. The main prerequisite is that an attacker controls several of the miners in the network. This may be achieved by using malware to capture and control their Mining Clients or by illegal collaboration of some miners. If that is the case, the attack may be successful even if the remaining miners are honest and their computational power is far greater than that of attacker and his allied miners. This situation means that an attacker is not capable of inserting the conflicting block in the blockchain, as in the case of the 51% attack.

This threat is executed as follows: suppose an attacker A wants to double spend the amount of bitcoins that he/she sent to some recipient R. In order to perform a successful race attack, an attacker A creates two transactions, denoted as Tx-A and Tx-R. Both transactions have the same input (hashes of the previous transactions from which bitcoins are being transferred), but different outputs (the amounts to be sent encrypted with public key of the recipient). If both transactions are executed simultaneously, they have an equal probability of being verified in the next block, as miners cannot accept two transactions with the same input fields. Therefore, only the transaction included in the block that reaches miners first will be accepted after verification. If some miners receive the block with the transaction Tx-R and the majority of miners receive the block with the transaction Tx-A, then the transaction Tx-A is more likely to be verified and included in the next block.

In this scenario it is necessary that the time at which the recipient receives the transaction Tx-R is shorter than the time at which the recipient receives the transaction Tx-A, what means that the transaction Tx-R should reach the recipient before the transaction Tx-A. If the recipient receives the transaction Tx-A earlier than the transaction Tx-R, then the recipient will first store the transaction Tx-A into his/her wallet and reject the transaction Tx-R. Hence, asking the attacker to reissue the payment transaction. After the attack is successful, the payment amount goes back to the attacker and by the time the recipient has realized that he/she has received an invalid transaction, the services paid by the transaction may already been completed.

Block Withholding Attack: This attack is known to be the most expensive double spending. Whenever a transaction is initiated, the sender sends it to the Bitcoin network, which broadcasts it to the entire network. A transaction is not confirmed until it is added to a block in the blockchain by the Bitcoin miners. This attack requires an attacker to be a fraudulent miner and in that case the attack is performed as follows: an attacker creates a conflicting transaction which sends some amount of bitcoins to the account owned by the attacker. The attacker does not release the block with such transaction what has as the consequence that the block is not included in the blockchain. The attacker then sends the same bitcoins to a recipient in order to pay for some services. In that moment, the attacker will release the withholding block what will cause the previous transaction to the recipient to be overridden by the one which pays bitcoins to the attacker.

6.3 Attacks by Miners – Selfish Mining

Bitcoin transactions are stored publicly in the Bitcoin blockchain. Many miners use their computational resources to verify the transactions by performing cryptographic computations. The generated block is then appended to the end of the block chain. Then, the miners keep on working on the next blocks. The more computing power and resources a miner spends, the greater is his/her chance to solve the hashing problem. Bitcoin miners usually work in groups and share the reward they receive, based on computational power that each miner contributes to the mining pool. The prerequisite (and the requirement) that this process is performed correctly and honestly is the core of the Bitcoin protocol.

A lot of research has been performed to analyze the behavior of Bitcoin miners and its influence to the reliability and correctness of the Bitcoin system ([Eyal, 2013], [Narayanan, 2013]). However, the development of the deployment activities for the Bitcoin system, especially in the area of mining arrangements, indicate very clearly that with the current status of the Bitcoin system mining is no longer completely decentralized. Namely, first, miners are partnering in mining pools and at the time of writing this Report there were only several dominant mining pools. In addition, there is the possibility that a large number of selfish miners can join a mining pool, comprising a group of miners who share the computational resources and with these resources control the system's mining power. This violates the decentralized nature of the Bitcoin protocol. As a result, such pools usually receive reward incentives that are larger than their fair share. This attack is called selfish mining.

Selfish mining attack is performed in the following way [Springer, 2014]: when one of the miners in a group of selfish miners find the correct value of the hash, he/she does not release the block back into the Bitcoin network immediately, but withholds it for some time. Since the block has not been released, all other miners keep on mining that current block. Without validating it they cannot move on to the next block. In the meantime, the selfish miners start working on the next block. When the remaining honest miners resolve the block that was

withheld by the group of selfish miners, in that moment they release the withheld block into the network. In that moment, selfish miners immediately also release all the blocks that they have validated in the meantime, what might be a group of several blocks. As the reward is assigned to the (pool of) miners that created longer block chain, selfish miners win over the honest miners and receive the reward.

The chances to receive such reward increase exponentially with the size of the group. Therefore, selfish miners usually try to add more miners into their group in order to increase their cumulative computational power. This snowball scenario helps them to avoid the situation in which the group of honest miners finds the block before the pool of selfish miners finds the next block, due to enhanced computational resources of the selfish mining pool. It has been realized that if one third of the total Bitcoin miners form a selfish mining group, they can control the mining process, resulting in compromise of the decentralized nature of the Bitcoin protocol. The selfish mining group can then control which miners can further participate in the mining process. Furthermore, they can also collect valuable information about which transactions are already committed and they can even "roll-back" the blockchain by inserting illegal blocks earlier added to the chain and recreating the rest of the blockchain.

6.4 Attacks on Users Anonymity

Initially, when the Bitcoin protocol was designed, it was claimed that the protocol provides complete anonymity of both the sender and the receiver of each payment transaction and that users cannot be traced in the Bitcoin system. But, several researchers have recently discovered the possibilities to identify the sender and the receiver of a transaction by using some additional computational power. Based on these results, the Bitcoin protocol is now considered to be pseudo-anonymous.

The approach to violate user's anonymity when making transactions is the following: in order to make a payment transaction, the sender has to create a key pair. The key pair comprises a public and a private key. The public key acts as an account identifier for incoming transactions and the private key is used to open the wallet and to sign the outgoing transactions. Each transaction has a list of its inputs and outputs. The input contains all previous transactions performed by the same user, so the miners can verify that the bitcoins used in the current transaction are not already spent (prevention of double spending). Transactions usually have two outputs: one specifies the receiver of the transaction while the other output contains the address of the sender. The address of the paying account is used as so-called *change address*, i.e. the remaining bitcoins in the account, after the payment amount, are returned ("paid") to the current account. The list of previous transactions, included as an input list in each transaction, can be used to create so-called transaction graph. These graphs can be used for tracking the sender by tracking the sequence of his/her previous transactions.

6.5 Malware Attacks

Attacks on Bitcoin Wallets: Bitcoin wallets are software modules and they use private keys to access bitcoins stored in the wallet. If the private key is compromised, all of the bitcoins in the wallet are lost. In order to attack the Bitcoin wallets, the attacker writes some malicious code and spreads it through the network as a botnet ([Blasco, 2013], [Mt.Gox, 2014]). If the wallet is infected by malware, the infected code can steal data, including the *wallet.dat* file from the computers where wallet is located. This attack, if successful, steals the bitcoins.

There is the possibility for users to encrypt their wallet files in order to prevent theft of bitcoins, but some malwares have capabilities to log key strokes and in that way steal the password and decrypt the required file. Some known malware attacks that use this method have been reported in the literature. Mt.Gox exchange was hacked using this type of the attack.

Mining Botnet Attacks: Apart from stealing bitcoins stored in wallets, some malwares are designed to attack the computational resources of different machines. As the miners receive rewards in the form of bitcoins for their successful mining process, they always try to increase their computational power, to get more and more rewards.

The attackers have now found a way to win this competition. They write a malicious code and spread it in the form of botnets. The code installs Bitcoin daemon on victim's machine and connects it to the mining pool. The attacker then uses victim's computational mining power to mine bitcoins. As the computation power is enhanced, the chances to win, by verifying blocks, is increased. Malware is spread through fake emails, Skype, and phishing websites.

All of the above described attacks are just the major types and are constantly being modified by attackers to launch new attacks.

7 Examples of Alternative Virtual Currencies

7.1 Alternative Crypto Currencies

This section describes different types of crypto currencies alternative to Bitcoin. They all belong to the category of crypto currencies because they are all generated and validated using computationally intensive cryptographic operations. In fact, they all represent the full analogy to Bitcoin and the only difference from Bitcoin is that they use their own instance of the blockchain and software components to perform and validate payments.

Virtual currencies alternative to Bitcoin may be created in two ways: by extending Bitcoin block chain with alternative branches (this approach is sometimes called "hard fork"). The essence of this approach is that the system that uses some alternative virtual currency still uses Bitcoin system distribution network and Bitcoin miners. The only difference with Bitcoin is that such systems have their own virtual currency, that currency has its own conversion value to the real-world currency, and the system has its own community of users.

In essence, other than being an alternative system and an alternative currency, such alternative payment systems do not have any significant differences and therefore advantages compared to the Bitcoin system. In fact, due to the popularity of the Bitcoin system and some of its deployment benefits, such systems handling alternative crypto currencies have even some disadvantages. One of the most important is their short blockchain, what has been shown in practice to be serious problem for any system using alternative "hard fork" blockchains to validate transactions [Ali, 2016].

Figure 4 presents the list of the top 50 cryptocurrencies by market capitalization [CC, 2016].

#	NAME	MARKET CAP	PRICE	AVAILABLE SUPPLY	24H VOLUME
1	Bitcoin	€12,160,200,711	€757.56	16,051,737 BTC	€63,107,631
2	Ethereum	€644,327,048	€7.40	87,069,625 ETH	€5,441,894
3	Ripple	€224,786,519	€0.006280	35,794,578,423 XRP *	€1,044,937
4	Litecoin	€171,001,165	€3.49	48,945,629 LTC	€1,761,291
5	Monero	€110,520,197	€8.14	13,578,448 XMR	€1,245,401
6	Ethereum Classic	€94,860,230	€1.09	87,006,731 ETC	€1,850,336
7	Dash	€67,927,243	€9.75	6,964,271 DASH	€1,883,521
8	MaidSafeCoin	€39,647,454	€0.087609	452,552,412 MAID *	€198,127
9	Steem	€35,196,788	€0.154010	228,535,972 STEEM	€55,447
10	NEM	€33,037,529	€0.003671	8,999,999,999 XEM *	€95,071
11	Augur	€31,931,831	€2.90	11,000,000 REP *	€154,998

12	Factom	€23,650,434	€2.70	8,753,219 FCT *	€652,574
13	Dogecoin	€22,515,741	€0.000210	107,349,290,302 DOGE	€181,296
14	Waves	€21,678,303	€0.216783	100,000,000 WAVES *	€30,601
15	Stellar Lumens	€18,989,926	€0.002744	6,921,534,188 XLM *	€132,975
16	Iconomi	€18,794,900	€0.216033	87,000,000 ICN *	€76,869
17	DigixDAO	€18,355,810	€9.18	2,000,000 DGD *	€15,813
18	Peerplays	€17,146,726	€17.15	1,000,000 PEERPLAYS *	€1,725
19	Lisk	€14,008,928	€0.140089	100,000,000 LSK *	€186,679
20	GameCredits	€12,630,852	€0.212647	59,398,275 GAME	€317,121
21	Ardor	€9,623,302	€0.009633	998,999,495 ARDR *	€8,150
22	BitShares	€9,467,319	€0.003672	2,577,920,000 BTS *	€76,584
23	Emercoin	€8,355,744	€0.213427	39,150,337 EMC	€32,148
24	Zcash	€8,281,348	€32.67	253,481 ZEC	€678,594
25	Gulden	€8,190,342	€0.024307	336,960,445 NLG **	€32,702
26	Golem Net Tokens	€7,718,991	€0.011335	681,009,001 GNT *	€6,259
27	Xaurum	€7,466,492	€0.083989	88,898,513 XAUR *	€16,534
28	ShadowCash	€7,279,916	€1.10	6,609,817 SDC *	€31,766
29	Bytecoin	€6,923,704	€0.000038	182,106,470,601 BCN	€372
30	Storjcoin X	€6,827,135	€0.135276	50,468,144 SJCX *	€4,965
31	Stratis	€6,695,065	€0.068181	98,195,961 STRAT	€146,044
32	Tether	€6,655,890	€0.957463	6,951,590 USDT *	€452,654
33	Bitcrystals	€6,293,021	€0.151193	41,622,441 BCY *	€39,997
34	AntShares	€5,643,814	€0.112876	50,000,000 ANS *	€34,935
35	Counterparty	€5,583,009	€2.13	2,620,941 XCP *	€8,925
36	Nxt	€5,403,395	€0.005409	998,999,983 NXT *	€32,522
37	Peercoin	€5,215,641	€0.219851	23,723,553 PPC	€10,004
38	SingularDTV	€5,121,177	€0.008535	600,000,000 SNGLS *	€7,270
39	Agoras Tokens	€4,716,756	€0.112304	42,000,000 AGRS *	€215
40	SysCoin	€4,335,097	€0.008821	491,473,623 SYS	€96,597

41	Siacoin	€4,304,549	€0.000200	21,516,912,597 SC	€27,811
42	Rubycoin	€4,273,114	€0.179486	23,807,502 RBY *	€943
43	I/O Coin	€4,198,419	€0.257590	16,298,838 IOC *	€609
44	YbCoin	€3,768,721	€1.25	3,016,741 YBC *	€227,026
45	BitcoinDark	€3,699,374	€2.87	1,288,862 BTCD	€1,044
46	Synereo	€3,134,016	€0.038101	82,256,324 AMP *	€56,283
47	Swiscoin	€3,105,794	€0.006545	474,502,405 SCN	€60,190
48	Global C. Reserve	€2,677,906	€0.026267	101,947,805 GCR *	€1,313
49	NAV Coin	€2,640,033	€0.043689	60,428,068 NAV *	€26,693
50	Namecoin	€2,513,491	€0.170563	14,736,400 NMC	€71,257

Figure 4. Top 50 Crypto Currencies by Market Cap (Dec 2016)

7.2 Alternative Virtual Currencies

In addition to different types of crypto currencies described in the previous section, there are some new and innovative ideas to generate and use virtual currencies that are not of the type of crypto currencies. The most common type of such currencies are virtual currencies that are generated by conversion of real-world currencies into virtual currencies. Some innovative ideas and initiatives even suggest to use various forms of tangible or intellectual assets, in the digital form, to make payments. One such idea is to use electric energy instead of monetary virtual currencies or even user's privacy as a compensation for accepting advertising and promotion announcements. Some other human activities are also suggested as source of virtual currencies.

In the comprehensive research study of security of virtual currencies [Kounelis, 2015], the following three approaches are suggested to generate and use virtual currencies:

(a) Perform some crypto operation and in that way receive reward for the computing power and results created by such operation;
(b) Create new amount of virtual currency by exchanging an equivalent amount of real-world currency; or
(c) Perform some task or service and as a reward get the corresponding amount of a specific currency.

Furthermore, research [Kounelis, 2015] has classified different types of virtual currencies not only by the way how they are generated, but also by the environment (community) in which it may be used:

"Virtual currencies can be classified into three main categories:

(a) ***Closed virtual currencies:*** *this type of currencies is generated and used mainly in virtual games. This is a currency used inside the game and is generated by performing tasks and missions, always in the game world. Usually such currencies do*

not have a real value and can be used only under the domain (within the game) where they were created.

(b) ***Closed virtual currencies that can be gained through real money.*** *Such currencies are similar to the above category with the difference that they are generated by actually paying them with real money. The virtual currency after the acquisition can only be used inside the domain for which it was purchased and cannot be exchanged back to real money. The best equivalent of this type of currency are various forms of digital gift cards.*

(c) ***Open virtual currencies.*** *These are virtual currencies that are alternative to real-world money currencies and can be used in the same way as real money. They have an exchange rate to all known real currencies and can be exchanged to and from real-world currencies at any time."*

Ether: Ether is virtual currency launched by the company Ethereum. The virtual currency is created by converting real-world currency into virtual currency. The idea of Ethereum company is to create distributed, community-based investment funds, where small investors can vote on investments based on the amount of virtual currency invested in the Ether virtual currency. Unfortunately, due to incorrect design and built-in bug, Ethereum blockchain was recently hacked, with significant damage of approximately $ 50 M.

Electric energy: One of the innovative ideas for use of blockchain and public ledgers is to trade electrical energy by individuals and small companies [UK, 2016]. The vision is to create European 'Energy Union' "*with citizens at its core, where citizens take ownership of the energy transition, benefit from new technologies to reduce their bills, participate actively in the market, and where vulnerable consumers are protected*". However, beyond simply transferring electric energy from individuals as producers to individuals as consumers, the system can also be used to perform payment transactions using electric energy as virtual currency. The value of the unit of electrical energy on the market would be the equivalent value of the electric energy units that can be exchanged for other types of goods and services.

Intellectual activities: One of the interesting ideas is to use intellectual activities to create and earn virtual currencies. In [Gadwa, 2015], the following such system has been described:

"A system and method is disclosed of attention-based crypto currency. Currency is generated or "mined" by a user listening, in one embodiment, to a streamed song, and upon listening to the entire selection, the user, the song artist, and the streaming host server are each allocated a portion of Attention Based Currency (ABC) according to a formula which may vary based upon several factors, including the popularity of the selection, the number of simultaneous listeners and the number of times the song has been streamed. The formula chosen can promote listening to lesser known artists. The ABC can be traded or redeemed for products or services".

Generalized virtual currencies: In [Kounelis, 2015] a generalized concept of different virtual currencies was introduced. It was based on the definition of such general concept from the [ECB, 2012] document: "a virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community".

Identities and Privacy Tokens: In [Muftic, 2014] and related research the idea of using users' identities and privacy attributes was suggested as a form of virtual currency. The concept is similar to the idea of using intellectual activities to obtain virtual currencies. In this case, the idea is the following: since users receive promotions and advertisements, for which

service provides generate revenue, service providers would compensate consumers, who agree to accept advertisements and announcements with some form of open or closed virtual currency.

In the prosed system user identities, credentials and locations (as results of tracking) and user profiles (as results of profiling) are used as a form of "virtual currency" by various service providers indirectly, through various forms of advertising. In this process users create virtual currency by their activities on the Web by visiting various Web sites and by executing various activities (replying to inquiries, creating "like" tags, etc.). Service providers "sell" to users various commercial information and in that way "collect" from them "payments" in the form of their identities and profiles as virtual currency ("cash–in"). Service providers "cash out" that virtual currency by selling it to various advertisers. The value of the virtual currency is a collective category for "merchants" and determined by auction for their customers.

One example of such operational system is the www.studentkaninen.se web site. The basic functionality and the purpose of the site is to link researchers and experiment participants in scientific healthcare research projects. Researchers who need participants in their research experiments advertise their projects and needs and individuals register for participation. The site does not generate revenue as compensation to its promotion activities, but by collecting and distributing to various health and pharmaceutical companies statistical information about the types of research projects, the types of participants, and other "personal" information. Thus, full personal security and privacy is guaranteed, while the reward for the site's services is in the form of compensation for statistical information.

8 References

[Ali, 2016] Ali, M., at al., "*Blockstack: Design and Implementation of a Global Naming System with Blockchains*", Proceedings of the 2016 USENIX Annual Technical Conference (USENIX ATC'16)

[Andreesen,2014] Andreesen, M., "*Why Bitcoin Matters*", The New York Times, 2014

[Bitcoin, 2009] Double-spending, "Double-spending".[online], https://en.bitcoin.it/wiki/Double-spending

[Bitcoin, 2010] https://bitcoin.org/en/how-it-works

[Bitcoin, 2016] https://en.bitcoin.it/wiki/Main_Page

[BitID, 2015] BitID, "*BitID Open Protocol*", http://bitid.bitcoin.blue/

[Blasco, 2013] Blasco, J., "How Cybercriminals are exploiting Bitcoin and other Virtual Currencies", 2013, http://www.alienvault.com/open-threatexchange/blog/how-cybercriminals-are-exploiting-bitcoin-andother-virtual-currencies

[CC, 2016] https://coinmarketcap.com/

[Drainville, 2012] Drainville, D., "*An Analysis of the Bitcoin Electronic Cash System*," 2012

[ECB, 2012] European Central Bank, "*Virtual Currency Schemes",* European Central Bank, 2012

[Eyal, 2013] Eyal, I., at al., "Majority is not enough: Bitcoin mining is vulnerable," arXiv preprint arXiv:1311.0243, 2013

[Franco, 2014] Franco, P., "Understanding Bitcoin: Cryptography, Engineering and Economics", John Wiley & Sons, 2014

[Gadwa, 2015] Gadwa, E., "*System and method for attention based currency*", U.S. Patent Application, 2015/0310474

[Karame, 2016] Karame, Gh., at al, "*Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*", NEC Laboratories Europe, Internal Report, 2016

[Kounelis, 2015] Kounelis, I., "*Secure and Trusted Mobile Commerce System based on Virtual Currencies*", Ph.D. Dissertation, The Royal Institute of Technology, Stockholm, Sweden, 2015

[Muftic, 2014] Muftic, S., "*Functional Infrastructure for Transactions using Digital or Virtual Currencies*", U.S. Patent and Trademark Office, Provisional Patent Application, August 2014

[Muftic, 2015] Muftic, S., "Security System for Virtual Currencies", presentation to JRC, Brussels, Belgium, 2015

[Muftic, 2016] Muftic, S., et al., "Business Information Exchange System with Security, Privacy and Anonymity", Hindawi Publishing Corporation, Special Issue of the Journal of Electrical and Computer Engineering, 2016, http://www.hindawi.com/journals/jece/2016/7093642/

[Mt.Gox, 2014] "*The Troubling Holes in Mt.Gox's Account of how it lost $ 600 Million in Bitcoins*", http://www.technologyreview.com/view/526161/the-troublingholes-in-mtgoxs-account-of-how-it-lost-600-million-in-bitcoins/

[Narayanan,2013] Narayanan, A., "*Why the Cornell Paper on Bitcoin Mining is important*", November 2013, https://freedom-to-tinker.com/blog/randomwalker/whythe-cornell-paper-on-bitcoin-mining-is-important/

[Perry, 2012] Perry, D., "*Bitcoin Attacks in Plain English*." 2012, [Online]. http://codinginmysleep.com/bitcoin-attacks-in-plainenglish/

[PoE, 2015] "*Proof of Existence*", https://proofofexistence.com/about

[Reid, 2012] Reid, F., et al., "*An Analysis of Anonymity in the Bitcoin System*", Clique Research Cluster, Complex & Adaptive Systems Laboratory, University College Dublin, Ireland, May 2012

[Sparkes, 2014] Sparkes, M., "*The coming digital anarchy*". In: *The Telegraph* (June 2014), http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html

[Springer, 2014] Springer, M., "*Is Bitcoin currently experiencing a Selfish Miner Attack?*" January 2014, http://scienceblogs.com/builtonfacts/2014/01/11/isbitcoin-currently-experiencing-a-selfish-miner-attack/

[Thomas, 2016] Thomas, S., at al., "*A Protocol for Interledger Payments*", White Paper, Ripple Labs, www.ripple.com

[UniCredit, 2016] UniCredit Bank, "*Blockchain Technology and Applications from a Financial Perspective*", Technical Report, Version 1.0, Data & Analytics, February 26, 2016

[UK, 2016] UK Government, Government Office of Science, "*Distributed Ledger Technology: beyond blockchain*", Report, 2016

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*): 00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the Internet.

It can be accessed through the Europa server *http://europa.eu*.

How to obtain EU publications

Our publications are available from EU Bookshop *(http://bookshop.europa.eu)*,

where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents.

You can obtain their contact details by sending a fax to (352) 29 29-42758.

European Commission

JRC 105207 – DG Joint Research Centre – Directorate E – Space Security and Migration

Title: Overview and Analysis of the Concept and Applications of Virtual Currencies

Author: Sead Muftic

Luxembourg: Publications Office of the European Union

2016 – 52 pp. – 21.0 x 29.7 cm

EUR 28386 EN – Scientific and Technical Research

series DOI 10.2788/16688 (online)

ISSN 1831-9424 (online)

ISBN 978-92-79-64826-7 (pdf)

Picture credits

All images copyright European Union except:

Frontpage : © zapp2photo – Fotolia.com

LB-NA-28386-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

Publications Office

doi:10.2788/16688
ISBN 978-92-79-64826-7