Bitcoin: Digital Illusion or a Currency of the Future?

Article *in* Financial and Economic Review · March 2020

DOI: 10.33893/FER.19.1.132153

2 authors:

Gyöngyi Bugár
University of Pecs
19 PUBLICATIONS **57** CITATIONS
SEE PROFILE

Márta Somogyvári
University of Pecs
12 PUBLICATIONS **31** CITATIONS
SEE PROFILE

Bitcoin: Digital Illusion or a Currency of the Future?*

Gyöngyi Bugár – Márta Somogyvári

Bitcoin has been one of the most interesting financial innovations in the last ten years. In this essay, we set out to discover why it has not spread as a medium of payment and how it has become a high-risk form of investment instead. We examine the operational mechanisms of bitcoin technology and explain the ideological background for the popularity of bitcoin. We conclude that, in its present form, bitcoin is not suitable to become a generally accepted medium of payment.

Journal of Economic Literature (JEL) codes: E42, G10, O31

Keywords: bitcoin, cryptocurrency, blockchain, libertarian economic policy

1. Introduction

The emergence of bitcoin and other cryptocurrencies may have been one of the most interesting financial innovations in the last decade. Originally intended as a medium of payment, this form of investment is now available to everyone both on-line and at bitcoin ATMs, which can be found in Budapest as well. Yet neither average users nor most finance professionals understand the ideology underlying bitcoin, the operational mechanisms and the risks inherent to this cryptocurrency. Our aim is to present the theoretical problem (double spending) that Nakamoto wished to tackle when he developed the blockchain system on which bitcoin is based; we will also outline the operational mechanisms of bitcoin and its role today. We also examine the ideological background that ensures the popularity of bitcoin and sustains the bitcoin community. Through our survey of these areas we hope to answer the question posed in the title and take a look at the future opportunities for using bitcoin. We then describe the white paper

* The papers in this issue contain the views of the authors which are not necessarily the same as the official views of the Magyar Nemzeti Bank.

Gyöngyi Bugár is an Associate Professor at the Institute of Management Sciences of the Faculty of Business and Economics at the University of Pécs. E-mail: bugar.gyongyi@ktk.pte.hu
Márta Somogyvári is an Associate Professor at the Institute of Management Sciences of the Faculty of Business and Economics at the University of Pécs. E-mail: somogyvari.marta@ktk.pte.hu

This research was financed by the Institutional Excellence in Higher Education Programme of the Ministry for Innovation and Technology within the framework of Pécs University's Topical Programme *No. 4* on *Increasing the Role of Hungarian Companies in Reindustrialising the Nation*.

The Hungarian manuscript was received on 14 September 2019.

DOI: http://doi.org/10.33893/FER.19.1.132153

serving as the technological background for bitcoin and the ideology underlying the cryptocurrencies; we also point out the importance of bitcoin. In *Chapter 3,* we describe the blockchain technology on which bitcoin is based, along with its operational mechanisms. In *Chapter 4,* we look at the role bitcoin plays in the economy as a medium of payment and as an investment opportunity. In *Chapter 5,* we highlight the constraints to its spread, due firstly to its technology and secondly to the regulatory environment. In conclusion, we summarise our insights into the future of bitcoin.

2. The development of the bitcoin system; the role and importance of bitcoin

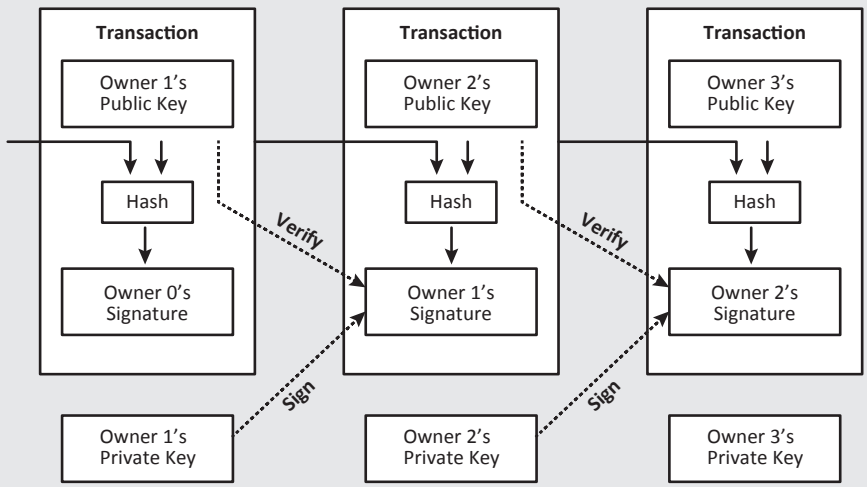
2.1. The Bitcoin White Paper: the development of a system

On 31 October 2008, *Satoshi Nakamoto* published his idea for a new innovative system of payments in a cryptography mailing list. Led by a sense of philanthropic mission, the author describes in his nine-page essay (published in the worst year of the last global financial crisis) an on-line network of payments that is free of any banks and central (mediating) authority, operates between independent and equal players and is in effect accessible by everybody (*Nakamoto 2008*). Bitcoin may be considered the very first conceptual design of all time for a system of decentralised, cryptography-based payments (*Gábor – Kiss 2018*).

The open-source-code system implemented as envisioned by Nakamoto is based on digital signatures rather than trust. The open source code makes the system public, so that anyone can freely enter and leave it at any time. The author defined the *bitcoins* created in the network as a *chain of digital signatures*. In a transaction, the holder of the electronic coin transfers it to the next holder by using their private key to digitally sign the hash[1] from the preceding transaction and the public key of the next holder, and attaches this to the end of the signature series representing the coin. Hash functions are processes used in informatics (essentially cryptographic algorithms) for converting data of any length to a particular length. The resulting final data will be called the hash (hash value). In fact, the hash is a check code identifying the original message, a kind of digital fingerprint[2]. The payee can check the digital signatures to confirm the proof. *Figure 1* demonstrates the sequence of transactions described above.

[1] A literal translation of the word 'hash' would be 'mince', 'chopped, ground meat'.
[2] József Schaffer: *Minden, amit a bitcoinról tudni akartál – végre magyarul is* (*All You Ever Wanted to Know about Bitcoin – Now Finally in Hungarian*). Electronic memorandum, 7 January 2014 http://plastik.hu/2014/01/07/a-bitcoin-ismertetoje/. Downloaded: 14 August 2019.

Figure 1
A chain of transactions for the transfer of bitcoins



Source: Edited from Nakamoto (*2008:2*)

A significant challenge in the operation of the system is to prevent amounts already spent from being spent again. To solve this problem, *Nakamoto* (*2008*) suggested the publication of transactions and transaction proofs based on consensus among the participants of the network. This removes the need for a central player to perform clearing and provide proof of transactions.

The transactions are published with the help of a distributed ledger, which is essentially a database that contains the transactions and is available to all participants. The data (individual transactions) in it are organised into blocks; the validated blocks constitute a chain (the blockchain). Individual nodes in the network compete to be the first to decrypt the next data block containing financial transactions and to supply it with a digital timestamp as proof. This involves decryption based on the use of a sufficiently difficult mathematical algorithm (proof-of-work). This provides proof that the participant of a particular transaction has not attempted to spend the amount in that transaction before.

Nakamoto (*2008*) calls the players competing for the transactions proof miners. Miners are motivated by the bitcoins they receive in return for decrypting the blocks. This is basically how money is created in the system: the transaction validators who decode the blocks are responsible for money creation.

Nakamoto (*2008:3*) describes the steps of operating the network as follows:

1) New transactions are broadcast to all nodes.

2) Each node collects new transactions into a block.

3) Each node starts to work on block decryption.

4) When a node has succeeded in decrypting the block, it broadcasts it to all the other nodes.

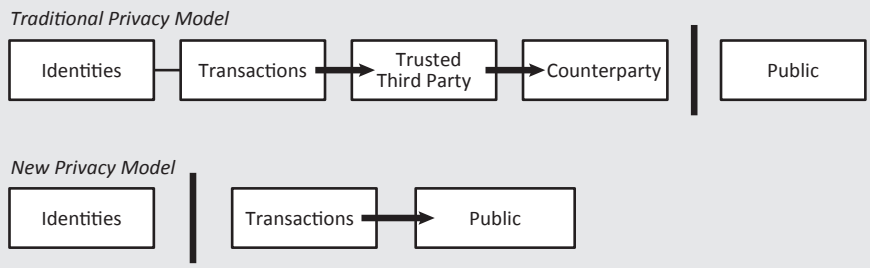
5) The nodes will accept the block only if all the transactions in it are found to be valid and there is no sign of any intention to spend an amount repeatedly.

6) Nodes express their acceptance of the block by starting to work on the next block in the chain through starting to use the hash value of the preceding, accepted block.

The secure operation of the system is guaranteed by the validation process based on the majority consensus of individual nodes. Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously to the other nodes, some nodes may receive one of these versions first, while other nodes receive the other one. In such a case, they will work on the first block they received, but save the other one in case the blockchain containing it becomes longer. It is always upon the decryption of the next block that it becomes clear which block is to be discarded, i.e. which branch is to be followed. (As a result, transactions in a shorter block version will not be executed and will need to be resubmitted.)

As regards the security of the system, *Nakamoto* (*2008*) highlighted the importance of the system of incentives within it. The first transaction of each block is a special transaction that creates new virtual money (bitcoin) that will become the property of the decryptor of the block. This incentivises the nodes to support the system and also ensures that virtual currency units enter into circulation. The 'remuneration' for the decryption of a block essentially serves as the return on the computer resources (CPU capacities) and the associated electricity expenditures. *Nakamoto* (*2008*) is convinced that a built-in incentive will ensure that system participants comply with the rules. If a greedy 'attacker' enters the network and possesses more CPU capacities than all of the honest nodes in total, then it may choose whether to take advantage of this and, misleading the system participants, reclaim all its former payments, or whether to use its resources to create new money. *Nakamoto* (*2008*) says that, in that case, it must recognise that it will be more profitable for it to respect 'the rules of the game', which will help it acquire more new bitcoins than all the other participants together.

Figure 2
Comparison of the traditional system of financial intermediation and the bitcoin confidentiality model



Source: Edited from Nakamoto (*2008:6*)

Nakamoto (*2008*) describes a system of payments that deviates from the traditional confidentiality model of banking in terms of the public disclosure of the transactions as well. In the traditional banking model, the participating parties and a Trusted Third Party (intermediary bank) have limited access to information, and a firewall completely excludes the public from the information flow. While the need to make transactions public makes it impossible to use the above model, personal data can still be protected; in fact, anonymity can be preserved by stopping the flow of information at a different point in the process. This is because public keys are not specific to individuals. Information about someone sending another person (identity) a particular sum is available publicly without making the transaction participants identifiable. This is similar to the confidentiality principles followed by stock markets, where the amount and the time of the transactions is published but the parties to the transaction are not disclosed. We demonstrate the difference between the two models in *Figure 2*.

2.2. The philosophies underlying bitcoin

Nakamoto's essay laying the foundations for bitcoin is seemingly a study of the technical problems of on-line payment systems, one that wishes to remove the banks and financial institutions from the payment process. But bitcoin and the cryptocurrencies have spread not due to the technology, but due to the ideology embodied in the technology. Two important components of this ideology are the questioning of regulation by any kind of government, including central banks and monetary governance, and a cyber-libertarianism that proclaims the primacy of the digital way of life.

It is a belief held in ultraconservative circles in the United States that the state is authoritarian (*Levin 2009*) and that any kind of government intervention, for

example social transfers and therein the automatic right to health insurance, will represent a breach of the freedom of the individual. These ideas regularly recur in bitcoin communities, which explains why bitcoin is a kind of movement and why it is able to convert more and more people into bitcoin believers. According to these ideas, all government should be rejected, only market forces are good and they can help prevent the concentration of power, which, if held by the state or the government, could lead to excessive power focus. They criticise the conduct of monetary policy and, based on conspiracy theories, the activities of the Fed and central banks (*Rothbard 2002, Mullins 1992*). According to these extreme views (see *Golumbia 2016*), inflation and deflation are not rooted in economic reasons, but rather in central banks' activities. This ideology lays the groundworks for creating money that is free from inflation through the bitcoin algorithm.

Cyber-libertarianism emphasises the primacy of the digital way of life; this is the only acceptable world view for not only the proponents of bitcoin but, often, for the participants of the digital world as well. One of the forms this takes is the defence of the absolute freedom of the internet. For cyber-libertarians, the only important, genuine expertise concerns digital technologies and since everything can be traced back to IT processes and IT-algorithms, if anyone does not understand these, they have no right to express an opinion (*Golumbia 2016*). Thus any criticism of bitcoin highlighting economic or social considerations will be disqualified in the eyes of bitcoin proponents.

2.3. The importance of bitcoin among cryptocurrencies

2.3.1. Types of cryptocurrency

The two main groups of cryptocurrencies are digital coins with their own blockchains and tokens building on existing blockchains. The first group itself is also normally subdivided into two. It includes bitcoin, which has been able to benefit from the innovative advantages of first entrants to a market and remains the most important cryptocurrency to this day, and alternative cryptocurrencies, altcoins, which are either descended from bitcoin or built on entirely new blockchain algorithms.

How can new cryptocurrencies be created from bitcoin? Bitcoin is built on blockchain software with an open source code and ledger, which means that there is an opportunity to change the software code. If there is disagreement in a blockchain community regarding such a change, the blockchain may split into two for good (this is called a 'fork'). Once it relies on the new code, the blockchain that was previously part of bitcoin will start to live a life independently of bitcoin. One of the purposes for changing the code is to add new features to the software; an example was the creation of litecoin, which increases the speed of the

transactions. It is also possible to introduce fundamental changes to the code, e.g. raising the size of blocks from 1MB to 8MB; this led to the emergence of bitcoin cash. There are also altcoins that are not descended from bitcoin, but are built on entirely new blockchains; examples are Omni, Ether and Ripple.

The other group of cryptocurrencies contains so-called tokens. Tokens do not have their own blockchains; instead, they use platforms (one example is Ethereum, which has its own altcoin called Ether) that allow for the creation of secondary digital 'cryptocurrency-equivalent' means using apps reliant on the platforms' own blockchain architectures (DApp). This process is much simpler than setting up a new blockchain. Coins are initially offered by announcing an ICO (Initial Coin Offering) in a White Paper. Tokens may represent a service that can be accessed in the event of the launch or the success of the project, i.e. the issuance of the token can be considered as a new form of crowdfunding; nevertheless, they are often purchased for investment purposes.

Popular tokens, whose price reaches several times their value at issuance, tend to be the ones aiming at an enhancement of blockchain technology. The objective of IOTA[3] is to accelerate transaction execution on the basis of a new philosophy, while NXt is intended to protect against attacks on cryptocurrencies with a proofing method. More than 90 per cent of the 1,394 tokens listed on the website cryptocompare.com lose their value quickly and are worth a fraction of their value at issuance after only a few months. According to some estimates, investors incurred USD 3.5 billion in losses on the collapse of PLUS Token, which was popular in Asia, especially in Korea and China, and offered 9–18 per cent interest per month in a kind of Ponzi scheme (*Emsley 2019*).

2.3.2. Market capitalisation of the most important cryptocurrencies

As of 24 August 2019, coinmarketcap.com had on record almost 2,500 cryptocurrencies. More and more cryptocurrencies are generated day after day, but most of these are relatively short-lived. Bitcoin is the biggest cryptocurrency, dominating the market at nearly 70 per cent, which, depending on prices, represents a market capitalisation of around USD 180 billion. The second biggest cryptocurrency after bitcoin is Ethereum, with USD 20 billion market capitalisation, while Ripple has USD 11 billion (this is a centralised blockchain that is concentrated in the hands of a single company and aims to accelerate interbank transfers). But what does market capitalisation expressed in USD mean in the case of a cryptocurrency? By definition, this is the quantity of cryptocurrencies (coins or tokens) in circulation, multiplied by the market price. This calculation method

[3] IOTA diverges from blockchains and uses graphs for proofing (DAG: Directed Acyclic Graph). As mining is not needed, the energy use of individual transactions is negligible and the system is much faster and more scalable than blockchain. Popov, S. (2018): *The Tangle Version 1.4.3*. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

copies the definition of the market capitalisation of securities. Since the indicators that are used to describe currencies (conversion rate, purchasing power, inflation, etc.) cannot be applied to cryptocurrencies, the very fact of using this indicator will question whether cryptocurrencies can be considered as money.

3. The technological background of bitcoin

3.1. Blockchain (ledger) technology

The blockchain is the main technological innovation of bitcoin.[4] It operates as a split, public ledger that records all bitcoin transactions. This ensures openness and transparency for all participants in the system. Essentially, the blockchain is a continually growing list of data blocks containing transactions, in which individual blocks are connected in a way that prevents forgery and tampering.

The digitally recorded data blocks are stored in a linear chain. The data blocks containing the transactions are encrypted (coded cryptographically) with a hash function and a time stamp is added. When a miner creates a new block, that block will contain the hash of the previous block and, as a result, the blocks will constitute a chronologically ordered chain (starting from the initially created 'genesis' block and ending with the most recent block). The network grows as this process is repeated over and over again.

Each block in the blockchain contains data (e.g. data about bitcoin transactions), a block header, a block identifier and a Merkle tree.

- The block header contains the metadata of the block.[5] These are the following: (a) the hash value of the block chronologically preceding the block; this serves the purpose of identifying the previous block; (b) the identification data of the miner decrypting the block; (c) the data structure capturing the transactions in the block, also referred to as the Merkle tree root.
- The block identifier is essentially the hash value that uniquely identifies the block.
- The purpose of the Merkle tree is to summarise the transactions in a block. 'Tree' is a term used in computing to describe a branching data structure. Merkle trees are normally shown upside down, with their 'roots' at the top and their 'leaves' at the bottom of the diagram. The role of the Merkle tree is to create an overall digital fingerprint from the transactions in the block, thus providing an

[4] In writing this section, we relied on two sources: information published on the website of Blockchain Technologies (https://www.blockchain-technologies.com) and an open publication book by Andreas M. Antonopoulos, 'Mastering Bitcoin', in a translation available electronically (https://bitcoinbook.info/wp-content/translations/hu/book.pdf).
[5] Metadata are data about data.

efficient process for checking whether a particular transaction is indeed included in a block. The Merkle tree is constructed by the recursive hashing of pairs of nodes until only one hash, the so-called Merkle root remains.

The most important characteristics of the bitcoin blockchain technology are the following:

- Consensus: all anonymous participants in the network agree to follow the rules of the network, i.e. they accept that 'there is only a single source of truth' in a blockchain environment.

This requires agreement from 51 per cent of participants. It follows therefore that a participant with sufficient computing capacities and 51 per cent of the nodes can hack the blockchain.

- Distributed data processing: there is no central node for the processing and distribution of data; all nodes can independently process and forward the proofed data to the network.
- Information storage capacity: the technology is able to record and keep the data of the transactions and the associated information.
- Identifiability of transaction origin: each transaction is recorded alongside the activity associated with it, so that it can be monitored in full.
- Non-alterability: no participant in the network may alter an already recorded transaction. Faulty records cannot be deleted and will remain visible at all times once recorded. Errors may be corrected only by submitting a new transaction offsetting the faulty transaction.
- Public access: all participants in the system may connect to the network without any constraints and may access the data stored in the blockchain.

3.2. SHA–256 algorithm

SHA is an acronym of Secure Hash Algorithm. This procedure is one of the most widely used hashing algorithms in cryptography. SHA is an overall name for the standard processes issued by the United States National Institute of Standards and Technology (NIST), one of which is the SHA–256 algorithm used for bitcoin. Although hash functions were first introduced to computing in the early 1950s, their real popularity may be dated to the late 1980s and the emergence of electronic signatures (*Buttyán – Vajda 2012*).

The first version of SHA (SHA 1) was developed in 1993 under the supervision of the United States agency responsible for radio signals intelligence technology (NSA: National Security Agency). This creates a 160-bit message digest, which

can then be used in the digital signature algorithm. The SHA–256 used for bitcoin operates along similar principles, but can manage significantly larger volumes of data. Its input (the message to be forwarded) may be $2^{64} – 1$ bit in length, which is subdivided into blocks of 512 bits during processing. The size of the output (the resulting hash value) is 256 bits long in total and comprises 8 blocks of 32 bits.[6] The denomination SHA–256 therefore refers to the bit size of the hash value received as an output from the algorithm.

3.3. Proof-of-work

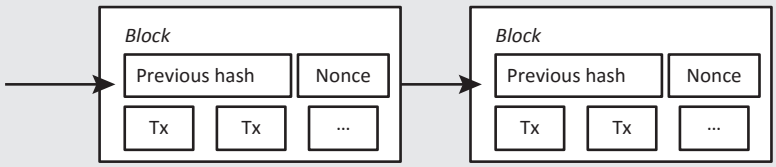
Proof-of-work is a numeric value that requires significant computing capacities to be generated. Bitcoin miners use the SHA algorithm to find a hash value that matches the level of difficulty applicable to the network as a whole (*Antonopoulos 2016*).

In the case of bitcoin, executing a proof-of-work entails searching for a value as mentioned above; applying the SHA–256 algorithm to that value returns a hash value starting with a certain number of zero bits. The step count of the algorithm is exponential in the number of zero bits required and can be verified by executing a single hash (*Nakamoto 2008*). Specifically, the miner decrypting the relevant block writes a value behind the previous hash (nonce) and then this nonce is incremented until the resulting hash value of the given block reaches the required number of zero bits (*Figure 3* illustrates the process). If the decryption is successful, the resulting new block can be altered only by performing the above work again. If new blocks join the chain in the meantime, then changing a particular block will also demand the decryption of all newer blocks following that particular block.

It is important to mention that, in addition to proof-of-work, the now increasingly popular proof-of-stake process is also used in the operation of cryptocurrency blockchain networks. In this case, the creator of the next block is selected by a combination of chance and wealth or age (stake).[7] It has the advantage of accelerating the operation of the system and eliminating the loss incurred by miners who start the calculations but do not receive bitcoins as someone else overtakes them. By contrast, with proof-of-work-based cryptocurrencies such as bitcoin, the creation of new blocks is based on mining, i.e. the successful execution of an algorithm with high computation requirements.

[6] For more detail on the above, see: *Kathi* (*2009*).
[7] https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Figure 3
The proof-of-work mechanism



Source: Edited from Nakamoto (*2008:3*)

3.4. The participants and the operation of the system

The key participants of the system operating the blockchain are called nodes, which may be miners or users. There is a high number of intermediaries relying on the above, which allows those with no computing knowledge or technical facilities to access the cryptocurrencies. In order for to submit and receive bitcoin transactions, users need an electronic wallet, which is normally a freely downloadable application. Transaction proofing is done on the computers of the miners and the resulting new block has to be accepted by the entire network. It is then attached to the previous block, thus increasing the size of the whole blockchain. Storing the entire blockchain on your computer is not necessary in order to take part in the network. In the first quarter of 2019, approximately 36 million users had access to cryptocurrencies such as bitcoin (*Tassev 2019*). By contrast, the number of computers (full nodes) that store the entire bitcoin blockchain stood at around 9,000 in August 2019 and has been gradually decreasing over the last two years.[8] The decrease is understandable; after all, there are no financial benefits from running the entire bitcoin blockchain, even as the number of blocks continues to rise. The size of the full blockchain, including the generic block, reached 226 GB in the first quarter of 2019. Most of those operating the entire node are not idealists rebelling against a monetary system overseen by governments and central banks but miners and investors. As the size of the blockchain grows, the proofing process carried out by the miners demands increasingly large computing capacities and specialised hardware and software. This has resulted in a process of concentration. The largest player on the market is the Chinese company BitMain, which is the largest specialised hardware producer and software developer and executes more than 20 per cent of bitcoin mining. By the start of 2019, a large proportion, approximately 70 per cent of energy-intensive mining was concentrated in China, specifically in areas where energy prices are low due to the underutilisation of

[8] https://bitnodes.earn.com/dashboard/?days=730

the electricity production capacities installed there (*Tuwiner 2019*). In 2019 the energy and other costs required for mining 1 bitcoin in China ranged between USD 507 and 4,562, depending on the price of electricity.[9] This situation will change in the future, however: after liquidating its cryptocurrency exchanges, China has listed mining as an undesirable activity and will most probably ban it (*Brenda – Alun 2019*).

There is an entire industry built on cryptocurrencies made up of service providers that allow the purchase of cryptocurrencies for 'real' national currencies and the trading of cryptocurrency at cryptocurrency exchanges, providing platforms for token issuance and the development of diverse applications; they maintain investors' accounts and analyse the exchange rates of the different cryptocurrencies.

As regards the regional spread of cryptocurrencies, 27 per cent of market players are concentrated in North America, where 18 per cent of the transactions take place and 39 per cent of the wallets are found. The second most important player is Europe, with significant growth also expected in the Asia Pacific region, especially Japan.[10]

4. The role and importance of bitcoin within the economy

4.1. Bitcoin as medium of payment

During its existence for more than a decade, bitcoin has not fulfilled its originally intended role. Paying with bitcoin has not become daily practice, and its acceptance as a medium of payment is rare. This is obviously due to its extreme exchange rate fluctuations. It is entirely understandable that merchants are not willing (or even able) to state the value of their products in a currency that does not have a stable exchange rate.

It should also be noted in this context that the lead time of bitcoin transactions is high compared to that of other payment methods (PayPal, credit cards). If the system is overloaded, this may greatly increase the transaction fees. This is important at the moment because, unlike with debit and credit card purchases, the transaction fee for a bitcoin payment is paid by the buyer (*Gábor – Kiss 2018*). With conditions like this, it is unlikely that the use of bitcoin will spread any time soon for buying small-ticket items (like a book or a cup of coffee).

[9] http://www.chinacryptonews.com/industry/chart-bitcoin-mining-cost-china-cheapest/
[10] https://www.fortunebusinessinsights.com/industry-reports/cryptocurrency-market-100149

There are still numerous uncertainties regarding the categorisation of bitcoin. The U.S. Commodity Futures Trading Commission (CFTC) defines it as a commodity, whereas the U.S. Internal Revenue Service (IRS) considers it an instrument that incorporates property rights. The U.S. Securities and Exchange Commission (SEC) categorises it as a security in certain cases (*Chohan 2017*), whereas the European Central Bank considers it a convertible decentralised virtual currency (*Gábor – Kiss 2018*, *Bánfi 2018*).

In their study of cryptocurrencies, *Gábor and Kiss* (*2018*) emphasise the misleading nature of the term cryptocurrency on the grounds that it could suggest that they constitute a subcategory of traditional currencies. They believe, and we agree with them completely, that they are in fact an entirely unique, new group of instruments.

4.2. Bitcoin as an investment

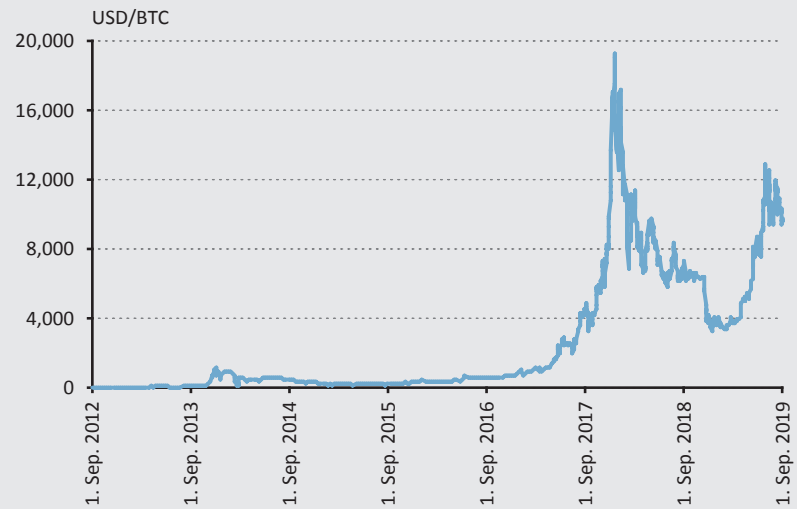
Since bitcoin is limited in its ability to function as money,[11] we should examine what opportunities it offers if we consider it as an investment asset. To see the changes in bitcoin exchange rates, we have downloaded its daily closing exchange rates against the dollar from the Yahoo Finance website for the seven-year period between 1 September 2012 and 1 September 2019. *Figure 4* presents the evolution of the exchange rate.

In the period examined, the daily bitcoin exchange rate rose from around USD 10 to USD 9,578, which is to say that it rose to around 960 times of its original rate. It should be remembered, however, that this extraordinary growth was coupled with outstandingly high volatility, i.e. extremely high risk. The graph shows clearly that the bitcoin exchange rate truly took off in 2017, when it rose from an initial rate of approx. USD 1,000 to above USD 19,340 (which is an annual return of about 1,900 per cent (!)).[12] The exchange rate then fell steeply, which bitcoin sceptics took as a sign of a 'burst bubble' (*András 2019*), but after a low point at around USD 3,000, it started to rise again and returned to values above USD 10,000.

[11] We do not discuss this question in detail in the present essay. We recommend reading *Bánfi* (*2018*) on the subject.

[12] In fact, bitcoin achieved the highest exchange rate of its history so far, namely 20,089 USD/BTC, on 17 December 2017 (https://coinmarketcap.com/currencies/bitcoin/historical-data/).

Figure 4
Bitcoin daily exchange rates between 1 September 2012 and 1 September 2019



Source: Edited from Yahoo Finance database[13]

Any assessment of bitcoin for investment purposes may rely on the combined assessment of its profitability and its risk profile. To this end, we first calculated daily returns from the daily exchange rate information available and then determined the annual effective return using the average daily returns in each individual year of the seven-year period. We used the standard deviations of returns to measure risk. In this case, we first used the time series of returns to calculate daily standard deviations for each of the years and then converted the resulting daily standard deviation values into annual values. We summarise our results in *Table 1*. We also state the return per unit of risk in the last row of the table.

[13] https://finance.yahoo.com/quote/BTC-USD/history?p=BTC-USD

Table 1
Changes in the effective average returns and risks of bitcoin between 1 September 2012 and 31 August 2019

Period	1/9/2012 – 31/8/2013	1/9/2013 – 31/8/2014	1/9/2014 – 31/8/2015	1/9/2015 – 31/8/2016	1/9/2016 – 31/8/2017	1/9/2017 – 31/8/2018	1/9/2018 – 31/8/2019
Annual Return (%)	2,294.27	11,741.89	-37.82	197.23	968.28	130.23	75.13
SD of Return (%)	102.95	390.02	71.53	57.61	71.19	97.9	73.54
Return/Risk	22.29	30.11	-0.53	3.42	13.60	1.33	1.02

Source: Calculated from Yahoo Finance database

Table 1 shows that both the returns and the associated risk values reflect the extreme fluctuation that already emerged from the historical exchange rate profile. Annual average returns ranged between –38 per cent and 11,742 per cent (the latter value is not a misprint and is equal to an average daily return of 1.3 per cent!). At the same time, the annual risk measured with the standard deviation of the returns ranged between 58 and 390 per cent. To compare: this measurement is generally between 10 and 20 per cent a year in the case of the S&P 500 share index (see *Misik 2018:70*). Return per unit of risk is, similarly to the Sharpe ratio, a measure of investment performance[14] and also ranges on a rather wide scale. In this case it takes values between –0.5 and 30.[15] Whereas the former points to losses from a falling exchange rate trend, the latter (outstandingly high) value reflects the impacts of the extremely high annual average returns. Even the associated extremely high risk failed to 'neutralise' the latter (cf. the values in *Table 1 Column 3*).

The above suggests that bitcoin is much more an instrument for speculation rather than a solid investment strategy ensuring balanced returns. A positive feature of investments in bitcoin is that its returns do not correlate with the returns of other instruments (equities, bonds, commodity market products, gold). Several authors (see e.g. *Brière et al. 2015* and *Misik 2018*) have pointed out this feature of bitcoin, which makes it suitable for offsetting the negative impacts of price falls of other instruments within an investment portfolio. Some studies have highlighted another positive characteristic, namely its ability to improve the efficiency of an investment portfolio (*Chen – Pandey 2014*; *Eisl et al. 2015*; *Misik 2018*). This means that adding bitcoin to the portfolio can help the resulting combination of investments achieve higher returns at the given level of risk thanks to the high returns of bitcoin per unit of risk, as shown above as well.

[14] More precisely, this ratio enables the comparison of the performance of various investments with different profitability and risk characteristics.
[15] It should be noted that *Misik's* (*2018*) analysis puts this indicator at 1.68 in the case of the S&P 500 share index. In the period he examines, he calculates a return value of 13.07 per unit of risk for bitcoin.

5. Limits to the spread of bitcoin

5.1. Technology and energy constraints

There is a fundamental obstacle to the future use of cryptocurrencies in the trilemma formulated by Ethereum creator Buterin, namely that cryptocurrencies cannot satisfy all three requirements of scalability, decentralisation and security at the same time. Scalability is prevented by the system of proof-of-work, which limits the number of transactions per minute. Although decentralisation would ensure security, the rising size of blocks and increasingly complicated computational tasks are bound to lead to a centralisation of mining and, as is clear from the data, of trade as well (*Roubini 2018*).

The most important aim in creating bitcoin technology was to increase the security of transactions in such a way that reliance on a financial intermediary such as banks becomes unnecessary as the system is designed to prevent fraud. This is ensured by the open source code and the ability to backtest the entire blockchain. This may have been so initially but ever since cryptocurrencies have been used by more than a small group of cyberlibertarians and programmers, it is an illusion to speak of such an opportunity of control for 36 million users. Instead of a bank controlled by society or government, users need to trust cryptocurrency traders, token issuers and DApp developers, which operate on the verge of the law and, as shown by bankruptcies and scandals, can disappear in an instant. For example, the codes running on the Ethereum platform contain 100 bugs per 1,000 lines (*Gerard 2017:96*). The development of cryptocurrencies is centralised, essentially 'the code is the law' (*Roubini 2018*), but this code can be changed at any time and simple users have no say in that. Even the blockchain system itself is not protected from attacks and if 51 per cent of the system is concentrated in one hand, there is an opportunity to retroactively alter blocks (*Farivar 2014)*.

The executability and speed of bitcoin transactions depends on whether there are enough miners to find proof. But mining will be worth it only if its costs do not exceed the prevailing market value of bitcoin. The annual average energy usage for bitcoin mining is 61 TWh,[16] which is equal to 130 per cent of the total annual electricity use of Hungary (*MAVIR 2019*). Beyond its high energy use, bitcoin has no link to actual economic events, unless a country were to introduce bitcoin as a national currency and general medium of payment. Since this is unlikely, the electricity used in bitcoin mining is wasted energy and causes indisputable damage to society and future generations. The manufacturing of the hardware needed in the bitcoin infrastructure, the construction of the buildings and energy supply systems and the high energy use of mining create a very high environmental

[16] https://cbeci.org/

burden even if the electricity is produced from renewable sources. There is no type of electricity production that does not damage the environment, does not use environmental resources and does not contribute to a decline in biodiversity.

5.2. Regulatory environment challenges

The regulatory environment of cryptocurrencies varies almost country by country, and ranges from a full ban to permission. China and India, the two most populous countries of the world have completely banned the use of cryptocurrencies. The Chinese government has also started to wind up the infrastructure and the industry serving cryptocurrencies, and as a last step in this process it has now declared cryptocurrency mining an undesirable activity, citing environmental protection as a reason. At the same time, the Chinese central bank is planning to issue its own cryptocurrency (CBDC - Central Bank Digital Currency), which will not be a decentralised currency based on peer-to-peer technology but involve a removal of all cash from circulation and the possibility of introducing control over financial transactions, or all transactions of its citizens (*Bloomberg 2018*).

In contrast to complete prohibition, there are countries where cryptocurrency exchanges can be operated subject to a permit; examples include Japan, South Korea and Luxembourg. Switzerland plays a special role: in Cripto-Valley, which is located in Canton Zug, tax allowances and other subsidies are provided to start-ups that work on cryptocurrencies and blockchain technologies and employ 3000 people. The 50 largest companies there have approximately USD 44 billion market capitalisation (*CVVC 2018*).

It reflects the uncertainties surrounding the use of bitcoin that regulations are still underdeveloped in the USA and the EU, the most important players in the trading of cryptocurrencies.

EU regulation[17] is focused on the prevention of money laundering and also requires the registration of cryptocurrency exchanges and cryptocurrency services in the relevant country. Although the opportunity to launder money appears obvious when it comes to cryptocurrencies, in practice this risk is low, as demonstrated by a risk assessment by the UK Treasury (*HM Treasury 2015*). Due to their exchange rate volatility and uncertain liquidity, it is currently not worth using cryptocurrencies for money laundering. Also, the anonymity of bitcoin transactions is an illusion. All transactions remain indelibly in the ledger and also leave a trace on the Internet. However, the theoretical possibility of money laundering is a great challenge for regulators. The fight against money laundering is traditionally based on the identification of clients by financial institutions subject to central control. New

[17] *5th Anti-Money Laundering Directive* (*2018/1080/COD*)

principles and technological solutions are now necessary in order to reduce the risk of money laundering with cryptocurrencies (*Campbell-Verduyn 2018*).

Other than the implementation of EU directives, Hungary does not have specific rules on cryptocurrencies at the moment. The Ministry of Finance does not consider bitcoin as money (*Fintechzone 2018*), whereas the Magyar Nemzeti Bank warns of the high risk inherent in 'virtual instruments usable for payment' (*MNB 2018*).

6. Does bitcoin have a future?

In the debates about bitcoin, a frequently raised proposition is that bitcoin does not have inherent value (*Brown 2019*), that the cryptocurrency is in fact 'built on thin air'. Indeed, bitcoin cannot be used for any other purposes, unlike gold or other asset making tools. Bitcoin is pure information and, in this respect, it can play the role of an absolute currency that is not tied to any physical embodiment (*Simmel 1900*). However, information will become money only if a community accepts it as such. This means that money is made money not by its inherent value but the fact that market participants attribute value to it; this could be interpreted as an external rather than an internal value.

What motivates bitcoin users to buy bitcoins and other cryptocurrencies? It is primarily the infrastructure surrounding bitcoin and the secondary services reliant on it, which allow everyone to join; the news in the media about bitcoin and cryptocurrencies; the uncertainty of regulation and the profit outlook. Today, bitcoin is primarily a means for short-term speculation, an investment instrument that has no underlying specific economic process or performance other than its rather high use of energy and resources. Only one thing matters for those buying bitcoins: the belief that there will be others in the near or more distant future to whom they can sell their cryptocurrency. Since bitcoin users are not tied to a specific economic community or country, the potential users who will maintain cryptocurrencies in the future could number billions, coming from the population of Internet users.

It will be impossible for bitcoin or any other decentralised cryptocurrency to spread as a general medium of payment partly due to the technological and security problems detailed above. Also, it is hard to imagine a government that would give up its right to issue money and thus to exercise monetary control. For companies, accepting bitcoin would entail huge risks, as its exchange rate volatility could eliminate the company's margins in a matter of minutes.

Mention must be made of the impact of bitcoin on the development of financial instruments (*Kerényi – Molnár 2017*). In certain cases, blockchain technology may be suitable for tracking financial, economic or even social trends, while the idea of digital money, proposed by bitcoin, may generate new financial innovations such as Libra, which Facebook wanted to introduce but has faced rather significant obstacles, or the USD-based digital currency for which Wal-Mart has filed for a patent.

Bitcoin has not fulfilled the role intended for it by Nakamoto. This is due to the fact that while the software architecture he developed offers a technical solution to certain problems, it disregards the economic processes underlying financial transactions. To answer the question posed in the title, we can state that, in its present form, bitcoin is not suitable to become a generally accepted medium of payment. The security system built into blockchain technology increases the lead time of transactions and it is therefore unable to compete with the widely used financial technology solutions. The service providers of the bitcoin industry (the exchanges and wallet providers) operate on the verge of the law and can disappear or be wound up by government intervention at any time. Most countries do not have adequate regulations regarding their operations and thus users and investors cannot rely on any kind of protection. The history of over one decade of bitcoin shows that, even though it has not spread widely, it may survive as a high-risk investment instrument in a narrow market segment.

References

András, B. (2019): *Hát nem arról volt szó, hogy összeomlik a bitcoin?* (*So Wasn't Bitcoin Supposed to Collapse?*) *Portfolio.hu – Online news portal*, 5 August. https://www.portfolio.hu/prof/20190805/hat-nem-arrol-volt-szo-hogy-osszeomlik-a-bitcoin-333275. Downloaded: 5 August 2019.

Antonopoulos, A.M. (2016): *Mastering Bitcoin* (trans. for Bitcoin developers). https://bitcoinbook.info/wp-content/translations/hu/book.pdf. Downloaded: 14 July 2019.

Bánfi, Z. (2018): *A bitcoinról pénzelméleti szempontból* (*Bitcoin from a Theory of Money Perspective*). Gazdaság és Pénzügy (Economy and Finance), 5(1): 2–30.

Bloomberg (2018): *China's Plan to Sideline Bitcoin*. https://www.bloomberg.com/news/articles/2018-12-13/china-s-plan-to-sideline-bitcoin. Downloaded: 5 August 2019

Brenda, G. – Alun, J. (2019): *China wants to ban bitcoin mining*. https://www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4. Downloaded: 5 August 2019

Brière, M. – Oosterlinck, K. – Szafarz, A. (2015): *Virtual currency, tangible return: Portfolio diversification with bitcoin*. Journal of Asset Management, 16(6): 365–373. https://doi.org/10.1057/jam.2015.5

Brown, C. (2019): *Bitcoin Has No Intrinsic Value — and That's Great*. (n.d.). https://medium.com/coinmonks/bitcoin-has-no-intrinsic-value-and-thats-great-e6994adbfe0f. Downloaded: 5 August 2019.

Buttyán, L. – Vajda, I. (2012): *Kriptográfia és alkalmazásai* (*Cryptography and its Uses*). Typotex.

Campbell-Verduyn, M. (2018): *Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance.* Crime, Law and Social Change, 69(2): 283–305. https://doi.org/10.1007/s10611-017-9756-5

Chen, W.Y. – Pandey, V.K. (2014): *The value of bitcoin in enhancing the efficiency of an investor's portfolio*. Journal of Financial Planning, 27(9): 44–52.

Chohan, U.W. (2017): *Assessing the Differences in Bitcoin & Other Cryptocurrency Legality across National Jurisdictions*. School of Business and Economics, University of New South Wales, Canberra Discussion Paper. https://doi.org/10.2139/ssrn.3042248

CVVC (2018): *The Crypto Valley's Top 50 Technology Partner. The Blockchain Industry in Switzerland & Liechtenstein analyzed and visualized.* https://www.coinpro.ch/wp-content/uploads/2019/07/CVVC-Top50-H1-2019.pdf. Downloaded: 3 February 2020.

Eisl, A. – Gasser, S. – Weinmayer, K. (2015): *Caveat emptor: Does bitcoin improve portfolio diversification?* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2408997

Emsley, J. (2019): *Alleged Bitcoin Ponzi scheme Plus Token could be liquidating billions of dollars in stolen crypto, says VC*. https://cryptoslate.com/alleged-bitcoin-ponzi-scheme-plus-token-could-be-liquidating-billions-of-dollars-in-stolen-crypto-says-vc/. Downloaded: 24 August 2019.

Farivar, C. (2014): *Bitcoin pool GHash.io commits to 40% hashrate limit after its 51% breach*. Ars Technica, 16 July.

Fintechzone (2018): *A Pénzügyminisztérium válasza a kriptovaluták szabályozásával kapcsolatban* (*Response by the Ministry of Finance regarding the regulation of cryptocurrencies*). https://fintechzone.hu/a-penzugyminiszterium-valasza-a-cryptocurrencyk-szabalyozasaval-kapcsolatban/. Downloaded: 24 August 2019.

Gábor, T. – Kiss, G.D. (2018): *Bevezetés a kriptovaluták világába* (*Introduction to the World of Cryptocurrencies*). Gazdaság és Pénzügy (Economy and Finance), 5(1): 31–65.

Gerard, D. (2017): *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum & Smart Contracts*. CreateSpace Independent Publishing Platform.

Golumbia, D. (2016): *The Politics of Bitcoin Software as Right-Wing Extremism*. University of Minnesota Press.

HM Treasury (2015): *UK national risk assessment of money laundering and terrorist financing*. Her Majesty's Treasury and Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/UK_NRA_October_2015_final_web.pdf. Downloaded: 12 January 2020.

Kathi, F. (2009): *Hash függvények* (*Hash Functions*). Dissertation, University of Debrecen, Faculty of Informatics. https://dea.lib.unideb.hu/dea/bitstream/handle/2437/90313/Szakdolgozat_KathiFerenc.pdf;jsessionid=B66004CEDC6B420308BC16C17D65FFA1?sequence=1. Downloaded: 12 December 2019.

Kerényi, Á. – Molnár, J. (2017): *The Impact of the FinTech Phenomenon – Radical Change Occurs in the Financial Sector?* Financial and Economic Review, 16(3): 32–50. http://doi.org/10.25201/FER.16.3.3250

Levin, M.R. (2009): *Liberty and Tyranny: A Conservative Manifesto*. New York: Simon and Schuster.

MAVIR (2019): *A teljes bruttó energiafelhasználás megoszlása* (*The Distribution of Total Gross Energy Usage*). http://www.mavir.hu/documents/10258/229275463/Előzetes+Termelésmegoszlás++2018+MavirHonlapra+HU+20190131.pdf. Downloaded: 12 July 2019.

Misik, S. (2018): *A bitcoin a portfólióelmélet tükrében* (*A Portfolio Theory Perspective of Bitcoin*). Gazdaság és Pénzügy (Economy and Finance), 5(1): 66–73.

MNB (2018): *Az MNB kockázatosnak tartja a fizetésre használható virtuális eszközöket, például a Bitcoint* (*The MNB Highlights Risks of Virtual Media of Payment Such as Bitcoin*). Press release, Magyar Nemzeti Bank. https://www.mnb.hu/archivum/Felugyelet/root/fooldal/topmenu/sajto/sajtokozlemenyek/bitcoin_kozl. Downloaded: 12 July 2019.

Mullins, E.C. (1992): *The World Order: Our Secret Rulers*. Published by Ezra Pound Institute of Civilization, Staunton, VA.

Nakamoto, S. (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*. White paper. 1-9. https://bitcoin.org/bitcoin.pdf. Downloaded: 15 April 2019.

Roubini, N. (2018): *Crypto is the Mother of All Scams and (Now Busted) Bubbles. While Blockchain Is The Most Over-Hyped Technology Ever, No Better than a Spreadsheet/Database*. https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf. Downloaded: 12 July 2019.

Rothbard, M. (2002): *A History of Money and Banking in the United States: The Colonial Era to World War II*. Auburn, Ala.: Mises Institute.

Simmel, G. (1900): *Philosophie des Geldes*. Leipzig: Duncker&Humboldt Verlag.

Tassev, L. (2019): *The Number of Cryptocurrency Wallet Users Keeps Rising*. https://news.bitcoin.com/the-number-of-cryptocurrency-wallet-users-keeps-rising/. Downloaded: 14 August 2019.

Tuwiner, J. (2019): *Bitcoin Mining in China*. https://www.buybitcoinworldwide.com/mining/china/. Downloaded: 14 August 2019.