AN INTRODUCTION TO THE WORLD OF CRYPTOCURRENCIES[1]

Tamás Gábor – Gábor Dávid Kiss

ABSTRACT

While in the first half of the 2010s, cryptocurrencies have been of interest only for innovators trading in IT and in particular programming, by now, the rapid spread of these digital coins cannot be avoided by either researchers or participants and regulators of the capital markets.

Despite growing media coverage on the rise of digital currencies and especially bitcoin, and whether we witness a bubble phenomenon, most economics and fintech professionals know little about these intriguing and mysterious currencies of no intrinsic value cloaked in computer codes, although many believe that they have the potential to change the monetary policy of the future.

The aim of this paper is to provide a comprehensive overview on the functioning of cryptocurrencies. We are going to highlight the importance of decentralised applications based on the blockchain technology, and in this context, the Bitcoin financial settlement network, paying special attention to the mania around bitcoin.[2]

As it requires comprehensive IT knowledge, we will introduce the underlying technology to readers only to the extent necessary for an understanding of how cryptocurrency systems integrate into financial markets and the economy.

A comparison will be made between the surge in cryptocurrency prices and certain historical exchange rate bubbles, followed by a discussion of the valuation of bitcoin as an asset having no real intrinsic value, and the limitations of its use. Finally, we will put cryptocurrencies as a new asset class under scrutiny and in the last section of our paper, using the GARCH, GJR-GARCH, TARCH and APARCH models, reveal that the market price of bitcoin to the US dollar does not depend on the price of any other money and capital market instrument, and as such, may be a viable option of portfolio diversification.

1 The statements within this study reflect the opinion and views of the authors. They should in no case be construed as investment advice.

The authors wish to thank cryptocurrency market expert *Gábor Vidák* for his invaluable comments made as reviewer of this study.

2 Depending on the context, Bitcoin may also refer to the protocol operating the Bitcoin system, the open source Bitcoin software or the community using the system in different sources. Neither the procedure of separating the terms Bitcoin and bitcoin is universally accepted." (see Ziád Bánfi (2018): *About bitcoin from the point of view of monetary theory. Economy and Finance*, 5(1), pp. 2–29

JEL codes: O30, E49, E59, C22

Keywords: bitcoin, ethereum, crypto, blockchain, decentralized network

1 INTRODUCTION

At the time of writing this paper, the online portal CoinMarketCap, which is probably the most up-to-date and accurate source of information on the market of cryptoassets, recorded 1,542 different cryptocurrencies. Most of these digital instruments may not be familiar to the majority of our readers. Some function as currencies and are referred to as 'currency' cryptocurrencies (e.g. Bitcoin, Litecoin, Monero, Dash, ZCash), while others, called 'utility' cryptocurrencies create an infrastructure for other blockchain-based applications (such as Ethereum and Filecoin). Finally, the last category includes cryptocurrencies providing services ('application' cryptocurrencies, e.g. Augur, ox and Steem). Although each 'crypto' is different, they all have something in common: the technology. Before we discuss currencies using cryptography and in particular bitcoin in more detail, first, 'decentralised applications' should be explained. Knowing what these are is the key to a full understanding of the concept behind cryptocurrencies.

Although recent media coverage on cryptoassets mainly focused on price movements, the original purpose of the technology was not to be used merely as a currency (payment instrument or medium of exchange). For a better explanation, let us consider the functions of the respective asset classes. Corporate bonds are used by companies, government bonds serve the purposes of governments and public bodies, and mortgage bonds those of real estate owners. In this respect, cryptocurrencies in fact make it possible to run decentralised applications.

Decentralised applications represent a totally new approach in the world of electronic services. As an unconventional, novel solution they allow for the creation, funding and operation of decentralised services of a top-down design without the involvement of a central authority. As such, they are radically different from our familiar standards.

Imagine the following: you have grown up in a rain forest and, one day, somebody comes to you with a cactus, claiming that it is a tree. How would you respond? Probably, you would smile and question its definition as a tree, since what is the point in storing so much moisture underneath that thick thorny flesh when there is plenty of water around?

People react most probably in a similar way upon hearing about decentralised applications.

1.1 Decentralised applications

Decentralised applications allow for the provision of services without the need for a central – intermediary – entity, or server.

November 2008 was probably the most critical period of the worst financial crisis and bank run of all times. It was in those days that a draft proposal[3] for a revolutionary new alternative to payment systems operated by central counterparties was circulated under the name (or pseudonym) '*Satoshi Nakamoto*'[4] on the mailing list Cryptography. The system he devised enables payments without relying on central banks, clearing houses or online intermediaries such as PayPal[5]. This was the first decentralised concept employing cryptography in history, which, in addition to the primary aim of making real-time payment transactions possible, had the purpose to create a distributed ledger which is independent of any central authority.

It should not come as a surprise that his publication of only nine pages was titled 'Bitcoin'. Satoshi looked for a possible way to establish a trusted settlement system from which the central authority known from classic textbooks that monitors, completes and settles cash flow as well as holds accounts for the parties is eliminated. He saw the greatest challenge in finding a solution to the problem of double spending, i.e. spending the same unit of money more than once. For data are intangible, i.e. they may be duplicated without limitation. Satoshi's main achievement was that he found a solution for what is called *'the Byzantine generals'* problem' in working his way through this challenge. In the case of distributed systems such as the Bitcoin network, data verification and time management are critical for the integrity and stability of the system. The Bitcoin protocol provides

3 Bitcoin: A Peer-to-Peer Electronic Cash System – Satoshi Nakamoto, satoshin@gmx.com, www.bitcoin.org

4 His identity remains a mystery to this day. Many believe that this is pseudonym, while others attribute the laying of the foundations of the bitcoin protocol to a narrow group. In Japanese, 'satoshi' means 'clear thinking', 'quick-witted' or 'wise'. 'Naka' stands for 'medium', 'relationship' or the 'inside' of something, while 'moto' could be translated as 'origin' or 'foundation'. These are very fitting terms for someone who has started a revolution by creating a well-conceived algorithm.

5 Satoshi was quite explicit about his intention to relieve – or replace? – the current banking system. He hid the following message in the genesis block, numbered block 0, of the Bitcoin protocol: 'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks', referring to an article published in *The Times* on 3 January 2009 about the British Chancellor of the Exchequer considering a second bailout. This leads to the conclusion that Satoshi essentially disapproved of central intervention and the asymmetry of bailouts, i.e. that banks scoop substantial profits when the system is doing well but in the event of turbulence they are saved at the taxpayers' expense. Bitcoin was his solution to these problems. Source: https://en.bitcoin.it/wiki/Genesis_block.

a solution for the greatest challenge in achieving a consensus, namely, how to transmit trustworthy information over an untrusted network.[6]

In addition to smooth data transmission, the validation of data is also a prerequisite for the operation of online settlement systems. Satoshi envisioned a peer-to-peer network of independent and equal parties, fully open to any member of the public. The party wishing to make a transfer reports this intention to all the participants of the public network, specifying the sum to be transferred as well as its own and the recipient's public address, among others. The party also assigns its private key, that is, its signature[7] to the transaction in evidence of its right of disposal over the sum concerned. The only thing left to ensure is that the same sum is not spent more than once. In present-day centralised settlement systems, this role is fulfilled by a central entity. What happens when there is no predetermined central entity? Satoshi put forward a goundbreaking proposal for the competitive validation of transactions. The fact that a party performing validation is certainly required for the validation of a transaction does not necessarily mean that it always has to be the same participant. Just as in market economies, participants must enter into competition. For this purpose, however, an additional component is needed: a reward that acts as an incentive for the parties to validate transactions. It was this incentive that Satoshi named 'bitcoin', while he called the competing participants of the validation process 'miners' by analogy with the gold miners of the past. By implementing an open source code, he created market economy conditions with free entry.

But how does this 'competition' actually look like?

Satoshi had a corresponding proposal. Imagine a long sequence of random numbers – called a hash[8] – which is extremely difficult to decode. So much so that only a pool of several thousand supercomputers is up to this task.

6 For more information on the Byzantine generals' problem see https://en.wikipedia.org/wiki/Byzantine_fault_tolerance and the study 'Automotive embedded systems' [Autóipari beágyazott rendszerek] by Fodor, D. and Speiser, F. (2014).

7 A so called Elliptic Curve Digital Signature Algorithm (ECDSA) is used for signing transactions. ECDSA is an asymmetric cryptographic process which allows for easy verification of the authenticity of a signature, but is extremely difficult to crack which is possible only with enormous computing capacities deployed. For more information see: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

8 Hash functions are used in information technology to map data of arbitrary size to fixed-length data. The output is called a 'hash'. Demand for such algorithms arose in the last years of the 1980s when electronic signature appeared. The SHA (Secure Hash Algorithm) is the most widely used and known cryptographic hash algorithm. Source: Wikipedia

Readers may have already asked the question: what is the use of such a seemingly complicated competition involving real costs[9] for the sole purpose of validating a transaction by decoding a sequence?

Competition for the validation of transactions, i.e. attaching a digital timestamp to them, is driven by personal gain under a reward scheme. Such competition based on the proof-of-work[10] concept ensures system-level stability and secure accounting of transfers. In this process, miners control each pending transaction and by doing so circumvent double-spending attempts by users, ensure compliance with all the rules and complete verifiable transactions, i.e. in the case of bitcoin, make the transfers. All this happens without a central settlement authority.

Let us shed more light on the proof-of-work concept with the thoughts of *Adam Smith*: 'It is not from the benevolence of the butcher, the brewer, or the baker that we expect our dinner, but from their regard to their own interest.' Cryptominers channel their resources into the appropriate hardware exclusively out of economic self-interest. Nevertheless, such self-interest is the guarantee for the functioning and stability of the whole system. Accordingly, one might say that the cryptocurrency and the underlying consensus are a manifestation of the 'invisible hand' of Bitcoin.

Miners sell part of the cryptocurrency obtained in exchange for their resources for hard currency on the open market[11] to cover the costs incurred in operating the requisite hardware (electricity, storage / rent, cooling). The remainder is their profit.

In summary, the instrument of reward at this marketplace of participants competing for the validation of transactions in place of a central settlement

9 Cryptocurrency mining requires state-of-the-art computer technology with a capacity to perform complex calculations, a powerful processor and/or even more powerful graphics cards (GPUs). The power consumption of such high-capacity computers is considerable. The price of a low-end computer built for mining purposes ranges between HUF 600,000 and 800,000 and consumes electricity of HUF 15,000 to 20,000 each month.
Today, dedicated hardware is used for mining bitcoins. A so called 'ASIC mining device' currently costs up to USD 4,000 or 5,000.

10 Miners are competing to be the first to solve a given data block which contain financial transactions and add it to the existing blockchain. To this end, they have to solve a mathematical problem of considerable difficulty as proof of work and evidence of acting in good faith. The more miners are competing on the network, the more difficult and time-consuming the mathematical problem will get. However, it will be just as difficult at all times to allow for a solution every 10 minutes. This serves a dual purpose: to determine who will get the reward for the solution and to filter out attempts at tampering with the ledger.

11 Specialised cryptocurrency exchanges have been set up for trading cryptocurrencies with each other and for fiat currencies. At the time of writing this paper, http://cryptocoincharts.info recorded a daily trading volume of USD 26 billion (inclusive of the value of cryptocurrency to cryptocurrency exchanges) on more than 130 cryptocurrency exchanges. Bitfinex, Bithumb, Poloniex, Bitstamp, Bitrex and Coinbase GDAX may be mentioned as the biggest and most widely known exchanges.

authority is the same instrument which, once traded, becomes an electronic payment instrument of digital monetary value, i.e. a cryptocurrency.

1.1.1 Decentralised services: Nothing new under the sun?

In fact, decentralised applications are in most cases employed in providing and using already existing services. However, they do so without the need for a central operator/provider.

For example, *Filecoin*[12], *Storj* or *Sia* enable us to store our data on the computers of a peer-to-peer network, without any central server(s) needed. Users looking for a secure cloud storage solution for their large data files would not pay a subscription fee to *Dropbox* or *Box.com* but rather to 'miners' in a peer-to-peer network who make their free space available on a voluntary basis and are rewarded with 'filecoins' in return. 'Filecoin', which is the 'token' of the network, may be traded for other cryptocurrencies or hard currencies on the exchanges.

Digital data storage solutions and electronic payment systems cannot be considered a novelty. What makes decentralised platforms innovative is that they do not have a company at their centre. The structures brought into existence this way represent a fundamentally new form of organisation.

A few words should also be said about Bitcoin's competition, Ethereum. Especially because it has seen an almost incredible, more than 10,000% price surge recently. Ethereum is a blockchain[13]-based decentralised network which creates an environment for running and operating other decentralised applications. As such, it has a prominent role and a dominant position among cryptocurrencies. Just like Bitcoin, the Ethereum protocol relies on an incentive scheme to invite the computing capacity needed for validating transactions. Miners receive 'ethers' in exchange for the resources made available. The innovative feature and appeal of Ethereum is that it provides a framework for the operation of different decentralised applications. It runs pre-specified smart contracts exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. It has to be mentioned at this point, that the irreversibility of transactions is not only an advantage but a drawback and a hazard at the same time. A bug in the code of a programme running on the Ethereum network may cause tremendous losses as it is not possible to recover the funds already transferred.[14]

12 The FileCoin project is among the first initiatives for a blockchain-based cloud storage solution. During the Initial Coin Offering in August 2017 more than USD 200 million was collected within an hour from institutional investors for the funding of the concept.

13 See the definition of blockchain below, in frames.

14 A similar incident occurred in the context of the DAO (decentralized autonomous organization) project in 2016, when 3.6 millions of ethers of a value of tens of millions of USD were stolen by exploiting a vulnerability in the code (contract). For more information see https://www.coindesk.com/understanding-dao-hack-journalists/

In most respects, decentralised applications in their current state are a long way from the traditional solutions used in our everyday lives. For instance, when comparing Bitcoin with PayPal or Filecoin with Dropbox, we may easily conclude that decentralised services often lag behind in speed, costs, scalability and user experience, in addition to a considerable uncertainty that their volatility entails. Nevertheless, they are characterised by a completely new feature, namely censorship resistance.

Censorship resistance means that everyone has unlimited access to the services at any time and the transactions made with them are unstoppable and immutable. Nobody may stop us from transferring bitcoins to the address of whomever we may choose. Similarly, we may run codes (smart contracts) on the Ethereum network or store data on the Filecoin platform without restrictions. Provided that we have Internet connection and as long as we pay the fee for the transaction – denominated in the cryptocurrency of the given system, of course – we may do as we please, free of external censorship or any imposition.

But which group(s) of people could find such a trade-off[15] acceptable?

For instance, people living in regions where certain services are not available or limited, or those who would like to avoid the attention of the authorities or any third party. Developing and emerging economies where the domestic currency loses value day by day due to hyperinflation (e.g. Venezuela) or where the combination of the financial infrastructure and the framework for capital regulation prevents the free(r) movement of capital across borders, and operators within the black and grey economy may be mentioned here. It should be added that with the continuous development of the protocol fewer difficulties are expected to occur in using the technology, which, as a result, will become suitable for wider everyday application.

What is a blockchain?

A blockchain is a distributed ledger, or in essence, a decentralised database of transactions, recorded in hundreds or thousands of computers. Data are divided into blocks, which are also assigned a unique identifier, a timestamp and a digital signature. New blocks are added to the chain by linking it to a previous block through a cryptographic procedure and being verified by peers. After verification, the databases of peers in the chain will be immutably and irreversibly updated.

15 It should be noted that a trade-off does not apply to those who buy cryptocurrencies solely for speculation purposes and not for tapping the potential of the technology.

2 THE BITCOIN MANIA

The leading article of the 21 December 2017 issue of *Fortune* magazine featured an interview with Nobel laureate for economic science *Robert Shiller*, who had warned about the overheated housing market on several occasions before the onset of the 2007–2008 subprime mortgage crisis in the United States. In this article, he shared his views about the price surge on the cryptocurrency market. He said: 'It seems like the dotcom bubble all over again, or the housing bubble all over again' (*Hackett–Wieczner*, 2017).

Let us take a closer look at this statement. There is a major difference between the two financial crises he mentions. While the latter culminated in a global financial crisis burning up assets of several thousands of billions of dollars and economic depression, together with State-funded bailouts to TBTF institutions[16] of unprecedented measures, the dotcom bubble emerging around the turn of the century left behind a significant technological legacy. For instance, national and cross-border fiber-optic communications networks were set up from the billions of dollars poured nonchalantly into the technology sector, which provided abundant funding also for research into 3G mobile communications technology. The dotcom bubble also contributed to the emergence of smartphones (Apple, Samsung), search engines using algorithms (Google), e-marketplaces (Amazon), social media platforms (Facebook, Twitter) or cloud-based IT solutions (Dropbox), not to mention regulatory changes of cardinal importance such as the 2002 Sarbanes–Oxley Act[17]. Just like the boom and bust economic crisis in the 1880s and 1890s (the 'Baring crisis') that left behind a nationwide railway network, the growing and bursting dotcom bubble also made a significant contribution to restructuring in the economy and technology.

Leverage should be highlighted as another substantial difference. While the dotcom bubble was inflated mainly by (stock) investments within retail and large investor portfolios, the radical increase of real estate prices was driven by demand

16 Too big to fail. A term used for institutions that are critical for the stability of the system. In the financial sector it is a source of moral hazard that large institutions define their business strategy safe in the knowledge that due to their size, the government will not let them fail and the bill of their excessive risk-taking will ultimately be footed by taxpayers.

17 The Sarbanes–Oxley Act of 2002 is regarded as the most significant amendment in federal securities regulation in the United States since the New Deal. The Act was adopted after a series of corporate financial scandals (including Enron, Arthur Andersen and WorldCom, among others). The most important provisions of the Act include the imposition of criminal and civil law penalties for infringements of securities regulations, regulations governing the oversight of auditor independence / internal auditing by external experts, executive compensation, insider trading and enhanced financial disclosures.

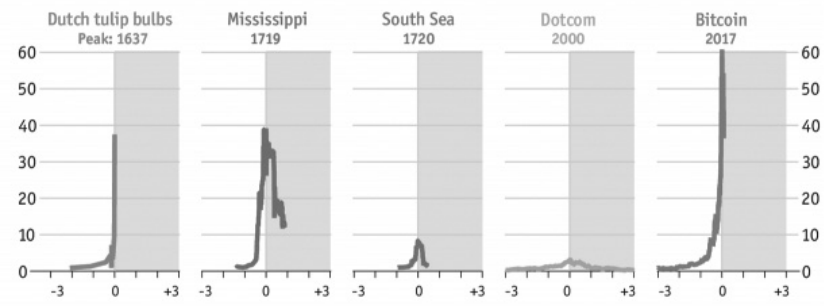
funded from extremely high leverage ratios[18]. The burst of the dotcom bubble did not involve any systemic risk since the exposure of the banking system was marginal. By contrast, the impact of deleveraging in the aftermath of the bursting housing bubble spread like wildfire first across the financial system and then it brought down the real economy as well.

In the light of the foregoing, we may consider the parallel drawn by Shiller between the 'irrational exuberance' on the cryptocurrency market and the dotcom and housing bubbles hasty and unfounded.

Mania is apparent, nonetheless. In 2017, the price of bitcoin and ether increased by 1.278% and 9.473%, respectively[19]. Figure 1 provides a good illustration of the magnitude of the increase on the bitcoin market in relation to asset bubbles in the past. It clearly shows that the price surge seen in the last three years is much more dynamic than the great price bubbles in economic history.

Figure 1

Comparison of historical asset bubbles



Note: The figure shows the increase over the starting price on the relevant exchange in the three years prior to the bursting of the bubble (or a shorter period where data for these years were not available), in percentages.
Source: Economist.com (Crypto-currencies are in a tailspin, 22.01.2018)

Based on the models for asset price increases presented in classic reference works and textbooks in economics, the increase observable on the cryptocurrency

18 Of course, micro- and macro-level circumstances also had a role in the emergence of the crisis, such as repeatedly repackaged, synthetic 'innovative financial products' created by quants, an extremely low interest rate climate and highly accommodative monetary policy, together with a regulatory framework that looked the other way too often.

19 The maximum increase within the same year was 2.100% and 11.400%. The cryptocurrency of Ripple, a company implementing private blockchain-based systems for interbank transactions, recorded an even more incredible increase: it soared by 353.843% to its peak in December 2017. (Let us stress that this is not a typo: we are talking about a 353-fold (!) increase.)

market could hardly be called anything else than a bubble. This is not much of a surprise either, considering that from preschoolers to the elderly, a growing number of people are occupied with bitcoin and the world of cryptocurrencies, even if only as a subject of discussion. According to a recent report by Google, in the category of 'how to' queries, 'how to buy bitcoin' took second and 'how to mine bitcoin' sixth place in their search statistics for 2017 (The Telegraph, 2017).[20]

Lively interest was also reflected in a vast increase in the number of newly registered users at cryptocurrency exchanges in the last quarter of 2017. Such an increase would pose a serious challenge for most exchanges in terms of technology and resources. Of the biggest cryptoexchanges, the US-based *Coinbase* (and its platform for corporate clients *GDAX*), *Bittrex* and *Kraken*, Luxembourg-based *Bitstamp* and Chinese *Binance* have recorded new registrations of the order of 100,000 daily during the last two months of 2017, respectively. After registering 250,000 new users the previous day[21], the CEO of *Binance* announced in a public statement on 4 January 2018 that they will temporary disable new user registrations[22] (Cointelegraph, 2018).

Based on the data on new registrations above, bigger exchanges have to cope with at least 1 to 3 million new clients increasing their client base monthly. Assuming that only one in three clients[23] deposits a smaller sum – e.g. USD 100 – on their account for investment purposes, from which they later buy a cryptocurrency, that would mean a daily capital influx of more than USD 3 million into the cryptocurrency markets – per exchange, it should be stressed. Although there are no official statistics available to date on investment into the crypto space, if we multiply that amount by the number of cryptocurrency exchanges of a higher trading volume and accepting hard currency payments, we arrive at the conclusion that tens of millions of USD flowed in fresh capital into the markets in the last months of 2017.

20 It is also interesting that 'what is bitcoin' was fifth on the list of most searched for 'what is' questions.

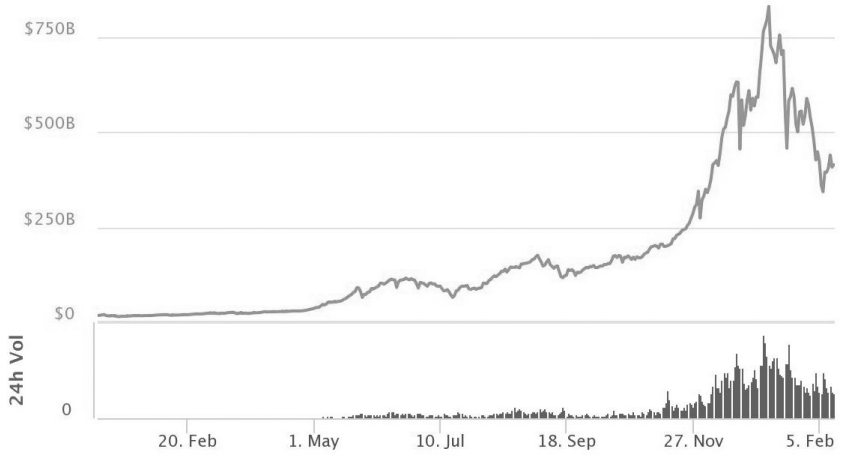
21 Despite their daily trading volume of several billions of dollars, high profit margin and abundant physical and human resources, cryptocurrency exchanges face a great challenge in complying with KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations imposed by the authorities. These require them to control and approve the documents submitted by each new client upon registration one-by-one and manually.

22 New registrations have been suspended on other cryptocurrency exchanges, too. For example, Bitfinex, Bitstamp and Bittrex did not receive new clients from December 2017 until Mid-January 2018.

23 We assume that 2/3 of the newly registered clients first take their time to get familiar with the platform.

Figure 2

Cryptocurrency market capitalisation, billion dollars 01.2017 – 02.2018



Note: Bitcoin's share of the total cryptocurrency market shrunk from 90–95% at the beginning of the year to about a third by the end of 2017.

Source: CoinMarketCap.com

The exponential growth of cryptocurrency market capitalisation observable on Figure 2 seems to corroborate our estimate of fresh capital inflow. Against this background, the unprecedented price surge in the last quarter of 2017 is less then surprising.

With respect to the price surge and in particular the increasing price of bitcoin, it should not be forgotten that in accordance with the consensus protocol of Bitcoin laid down in 2009 the supply of bitcoins increases steadily, though at a decreasing rate. The number of bitcoins in circulation grew by about 4% in 2017. Under current conditions, assuming a block time of around 10 minutes and a 12.5 bitcoin reward per block, ca. 1,800 new bitcoins are mined each day. Part of these is with all certainty sold for hard currency to fund maintenance and operating costs. With this daily output, at the current bitcoin price of USD 8,400[24], the value of new bitcoins going into circulation every day is USD 15,120,000. An inflow of fresh capital of the same volume to the Bitcoin market would be required for the upward trend to continue.

Figure 2 reveals more than development of the market capitalisation of Bitcoin. The dominant total market share of bitcoin (95%) at the beginning of 2017 has

24 Date of data collection: 11.02.2018

dropped to only one third of total market capitalisation over the year. This was due to increasing popularity of currencies on the altcoin market. The reason behind this shift was partly that, seeing the horizontal path of bitcoin during the summer of 2017, investors accustomed to multiple-digit returns reallocated part of their investments into these cryptocurrencies, which came into the spotlight precisely in that period and offered more attractive returns. Also, as a result of the mania surrounding the market, tremendous amounts of new funds were directed to altcoins.

In addition to altcoin investments, we should also mention the newest form of crowdfunding, i.e. ICOs[25]. During initial coin offerings, investors spend billions of dollars to fund plans, which in many cases cannot even be called a business plan, for projects often still at a conceptual level, summarised on a few pages in what is called a *white paper*. According to the report of CoinDesk for the last quarter of 2017[26], over three months, investors poured USD 3.23 billion into this highly speculative segment of the market, expecting that the price of the tokens would soar after they had been admitted to listing on an exchange.

Moving towards the end of the year, the cryptohype was fuelled further by news of an announcement by the two most significant American exchanges *CME* and *CBOE*[27] that they are going to include the eagerly awaited bitcoin futures product into their product range[28]. This opened the way for institutional investors, earlier excluded due to regulatory restrictions, to what was now a regulated liquid cash settlement market. Although institutional capital attracted by the regulated market following the introduction of bitcoin futures does not have a direct effect on spot prices, many believe that as trading volume and market depth grows, with due time, forward prices will be able to smooth sharp and unusually high volatility on the spot market. This would bring bitcoin closer to functioning more

25 The abbreviation 'ICO' stands for Initial Coin Offering. It could be described in simple terms as a unique combination of crowdfunding and initial public offerings (IPOs). Their aim is to raise capital for a project or for starting up a company by issuing a cryptocurrency. They are similar to IPOs inasmuch a share (stocks) or expected earnings are offered in exchange for the resources made available. Just like in the case of crowdfunding, investors get their money back if the minimum amount to be raised cannot be collected during the public offering. This form of public offerings is actually a response to the behaviour of venture capital and angel capital. Obtaining funds from these sources is quite difficult and lengthy for bitcoin startups. Many bitcoin and blockchain projects cannot meet the strict conditions attached to raising capital in the first place. For most, listing on an exchange is inconceivable. Source: http:// http://fintechzone.hu

26 CoinDesk: State of Blockchain 2018, 2017-Q4 Report, http://ww.coindesk.com

27 The Chicago Mercantile Exchange (CME) is the world's largest futures exchange and the Chicago Board Options Exchange (CBOE) is the largest options exchange in the US. Both institutions launched cash-settled bitcoin futures in December 2017.

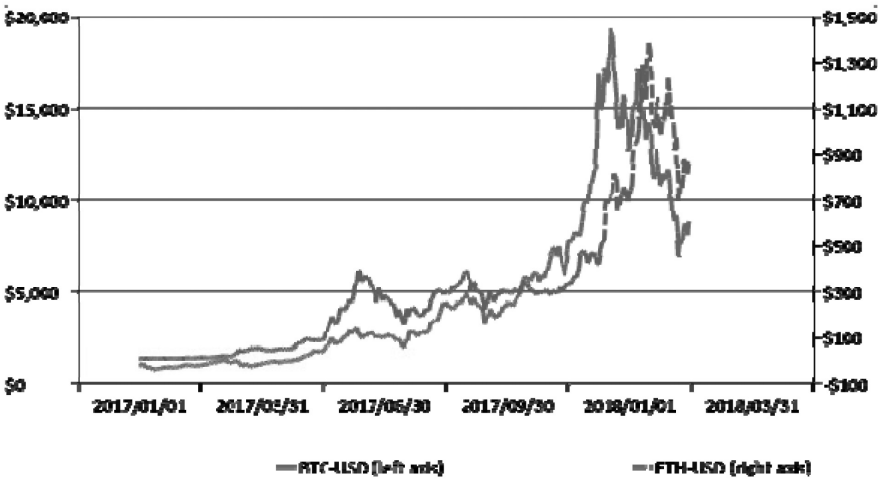
28 After CBO and CME, Nasdaq also announced that they are looking into the possibility of offering bitcoin futures from the first half of 2018.

effectively as a medium of exchange and a payment instrument. Such anticipations, as a matter of course, encourage further investors to enter the bitcoin spot market.

Nonetheless, an increase of several 1000% within the same year cannot be reasonably considered normal or the extreme risks it entails overlooked. Investors to bitcoin or any other cryptocurrencies should be aware of the substantial risk they take and that their investment is more like gambling than investing in an asset relying on tangibles. However, those who find the right entry point and prudently allocate only a small part of their investment portfolio to the cryptomarket may be lucky enough to realise extremely high returns. It goes without saying that a wrong choice of positions may easily lead to loss of the total amount invested.

There certainly is a mania. A mania that originates partly in people's blind faith in technology and partly in the fundamental human flaw of greed, driven by a fear of missing out on something (FOMO[29]). We are undeniably witnessing a bubble phenomenon. A bubble that had already begun deflating when this paper was written. The price of bitcoin dropped by almost 70% (~ 19,800 USD) within one and a half months compared to its peak in December 2017, while the price of ether, which back in the early weeks of 2018 almost doubled in 10 days (soaring from USD 750 to USD 1,400) shrunk by 55% in only 4 days (Figure 3).

Figure 3
Movements in the price of bitcoin and ether (01.01.2017–12.02.2018)



29 Although the term 'FOMO' (Fear of Missing Out) is very recent, the phenomenon which it describes isn't. It is an emotional response that is as old as humanity and an apt description of how investors were thinking in periods of financial bubbles. It is most closely associated with greed and hunger for more.

In our assessment, cryptocurrencies as high-risk investment vehicles are in an early stage of adoption. It would be difficult to predict which of them will vanish and which of them will be the frontrunners of the technology in the long term. It cannot be said with certainty either whether bitcoin belongs in the second group, since the new tech solutions that appear almost every day and modifications in the underlying protocols of existing instruments may easily redraw the current landscape of the cryptocurrency market.

One thing, however, is certain: Robert Schiller is wrong to compare the cryptocurrency bubble to the 2007–2008 subprime mortgage crisis. We believe instead that the cryptocurrency bubble will be interpreted as a milestone in the history of projects using the blockchain technology in retrospect, and in this respect, it resembles the dotcom bubble more closely.

2.1 The valuation of bitcoin

Every financial bubble involves a (false) assumption about the value of the asset concerned. A bubble emerges when the price determined by the interaction of supply and demand starts to move away from the intrinsic value of the asset derived from the tangibles at its basis[30].

However, in the case of bitcoin and other cryptocurrencies intrinsic value is not applicable. For the same reason, it is difficult to predict bubble phenomena as well. In the following, we will examine the factors that determine the value of bitcoin and other cryptoassets.

A number of scientific and less-scientific works have been written on this topic, but to date there is no consensus on the methodology to be applied for valuation.

Some believe that the price of cryptocurrencies is defined by supply and demand exclusively, while others propose that the unit 'production' cost of bitcoin should be calculated on the basis of the purchase price of current mining hardware (*ASIC – AntMiner S9*) and electricity costs, taking into account the level of difficulty of mining and the total computing capacity of the network (expressed in Gigahash/second). According to Trubetskoy, G. (2017), in September 2017, the electricity bill of mining 1 bitcoin was USD 1,567, calculated at the average unit price of electricity in the USA. However, his calculations do not include either the purchase price of the dedicated hardware, which went up to USD 4,000–5,000 due to a drastic increase in demand, or additional costs related to storage, maintenance and often cooling.

30 The fundamental value of an investment asset is determined by the economic performance of the company, institution or country issuing it and the discounted expected return of the asset.

There is another hypothesis based on which the value of bitcoin is defined relative to transaction volume, i.e. the more people use bitcoin for payments the higher value it represents.

The value of bitcoin cannot be grasped in tangible terms as it is not backed up by the economic power or performance of a country or the profit-making capacity of a company, and no stable-value assets are used to collateralise it. Those who believe that bitcoin is similar to stocks, i.e. one should buy some and later sell at a higher price, do not understand either what bitcoin really is or how corporate stocks work. For the stocks bought represent a share or ownership in a company and grant investors voting rights at the company's general assembly as well as a part – proportionate to their holding, of course – of the company's profits in the form of dividends. When the company is profitable, stock prices will increase as the dividends to be paid are priced in by the market.

There is no performance or intrinsic value that underlies the price of bitcoin. Instead, it has as its fundament the community consensus of the Bitcoin network. It is the common accord and shared faith of core developers, the mining pool, cryptocurrency exchanges and commercially interested parties that the digital code produced using cryptography – and existing only in the digital world – does have an intrinsic value. This value originates in the revolutionary concept of enabling rapid and cheap transactions, i.e. the transfer of assets between the parties, without the need for a third party or intermediary.

After all, it was also the result of a consensus that gold could be used as money several centuries before Christ. We can find references to this glittering yellow rare metal by Aristotle and Plato. They believed that it is connected to water – which is a logical assumption, since it was first found in streams – and is actually the combination of water and sunlight in a condensed form. Since the powerful rays of the sun were considered to be of a superhuman or divine origin, special importance was attributed to gold as well. Due to this belief and the fact that it was a commodity that had all the necessary properties to function as money (durable, divisible, homogeneous, transportable, generally accepted), gold and golden coins over time became a payment instrument.

In our increasingly digitalised world, where sooner or later all – technical – instruments will be able to communicate with us and with each other via the Internet, the thought of a fully digital currency used for everyday transactions is far from utopian or heretical. And if all this would become a reality, why should not cryptocurrencies have a part in this revolutionary change?

Of course, we will not make an attempt at answering these questions within the limits of this paper. We merely wanted to provide our readers with some food for thought.

2.2 The limitations of Bitcoin

Satoshi Nakamoto envisioned a digital financial system in the midst of the greatest global financial crisis of our times, which allows for a quick transfer of funds in real time at a very low cost. The timing of his paper was presumably not by accident, because the financial crisis sweeping through the whole world economy revealed the weak points of monetary policies and the deficiencies of an asymmetric key currency system.

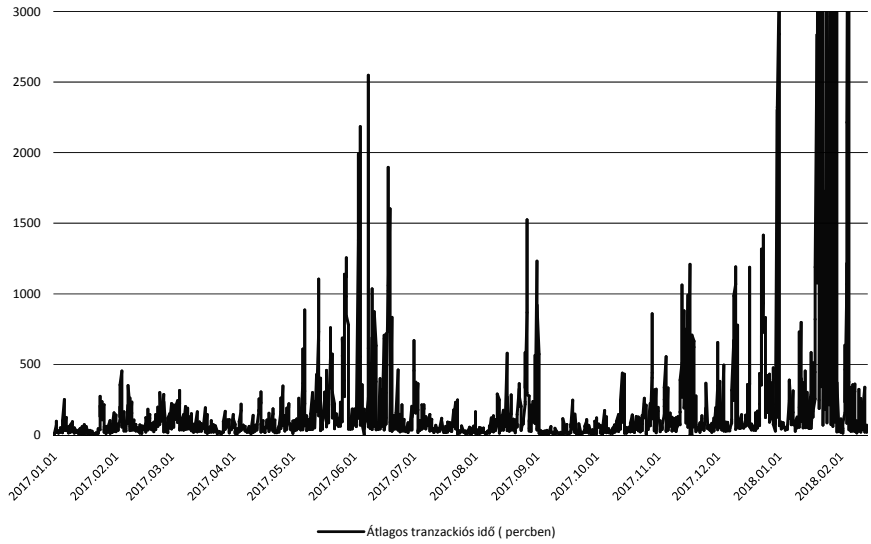
One of the main goals of his concept was, in fact, to create a digital payment system that is independent of monetary policies. No authority is able to regulate the supply of bitcoin, to redistribute it and to influence payments, and as such, it is completely independent of events in the world economy and world politics. However exciting and revolutionary new the settlement system of bitcoin appears, users have to face a number of issues and limitations today.

The bitcoin network became overwhelmed as a result of high interest in it in the second half of 2017. All this manifested itself in more expensive transfers and longer confirmation times[31]. Figure 4 shows the development of the average confirmation time since the beginning of 2017, which illustrates well the increasing waiting time. In January 2018, it occurred several times that bitcoin transactions were completed over a processing time of more than two days. The longest confirmation time to date was 11,453 minutes, i.e. nearly 8 days, completed on 23 January 2018. At present, for orders where people are willing to pay a higher transaction fee to miners, the median confirmation time is 13 to 15 minutes. Therefore, a trade-off can be observed between confirmation times and transaction fees. The peer-to-peer network will complete the transfer sooner for those who agree to pay a higher fee. This, however, is totally contrary to the concept laid down by the founder: the possibility of lightning-fast and low-cost digital transfer of money. Figure 5 shows the size of the memory pool ('mempool') queuing the transactions broadcast to the network, as a result of which the average processing time of transactions that were previously completed within a few seconds may extend even to hours.

31 The transaction fee payable for the transfer of bitcoins was a few cents in total before 2017. In the second half of 2017, however, as a result of the increasing load on the network, higher and higher fees (USD 1 to 5) had to be paid to the miners for the validation of transactions. There were 2 days in December 2017 before the holiday season when (presumably as a result of a load intentionally placed on the network) transaction charges skyrocketed: USD 55 had to paid on average even for transferring USD 10 worth of bitcoin (it even occurred in an extreme case that USD 162 (!) was paid for a single transaction). The transfer orders of those who did not want to pay such high fee were sent to the memory pool. If they were lucky, the order was fulfilled even at the lower fee they had specified. If not, their transfer orders were rejected.

We could already witness a number of attempts to increase the block size of Bitcoin and to reduce its block time; however, they have led only to 'hard-forks'[32] to date, leaving the original rules of Bitcoin unchanged.

Figure 4



Note: Confirmation times over 3,000 minutes were cut off to allow for a better view of the diagram.
Source: authors' elaboration based on data from http://blockchain.info

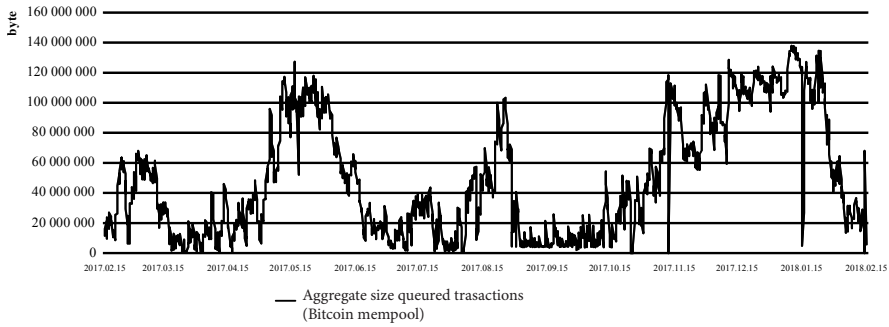
Although it is not our aim to go into technical details, we consider it necessary to say a few words about the protocol of bitcoin. According to the original protocol rules laid down in 2009 and fundamentally unchanged ever since, the block size was set at 1 Mbyte. Years ago, in 2010, the network infrastructure (bandwidth) at the time did not allow a larger block size to be used. Recognising this, in order to ensure stability, Satoshi introduced the block size of 1 Mbyte through a system upgrade.

32 Considering that the source code of bitcoin is open, anyone may copy it and make small or large modifications to it. Practically, a new blockchain is created through these changes. This is called a 'hard fork'. In this case, some of the miners switch to another blockchain and the validation (mining) of the transactions on that blockchain. During this process, the bitcoins are completely secure, because most such events are nothing else but developments or updates to the bitcoin protocol. There are updates, however, that affect the fundamental properties of bitcoin, such as its block size. In this case, by creating two blockchains, practically another digital instrument is created. Bitcoin owners may have access to their cryptocurrencies through both blockchains using their private keys. Such an event occurred on the Bitcoin network in August 2017, when Bitcoin Cash was created through a change of the block size to 8 Mbytes. People in the larger camp, who did not accept this change, were afraid that an increase in the block size would jeopardise decentralisation in the long term, since the larger block size would lead to certain players being pushed out of the market.

It is known from historical data that the size of an average bitcoin transaction is 495 bytes. That is, about 2,020 transactions can be placed in a 1,000,000-byte block. Considering that the protocol of bitcoin was defined in such a way that the degree of difficulty of the network should change, taking into account the total computing capacity, in such a way that the processing (mining) time of a block should be about 10 minutes, it is possible to carry out 3.37 transactions per second in total. This is a surprisingly low value compared to the nearly 500 transactions per second of PayPal and the 1,667 transactions per second of the VISA network.

The significant increase in the transaction time shown in Figure 4 resulted from the piling up of bitcoin transactions (Figure 5). The reason for this was that major players in the network (miners and developers) did not reach a consensus in the last 2 years on the development of the rules of Bitcoin and how network capacity could be increased in such a way that it does not jeopardise its foundations (decentralisation, transparency, censorship and tamper resistance).[33] At the same time, this is solid proof of the fact how democratically the system works, since decisions on key issues are made only very slowly and with full consensus.[34]

Figure 5
Aggregate size of pending bitcoin transactions, in bytes



Source: authors' elaboration based on data from http://blockchain.info

33 Serious technical debate has been going on for more than two-years between the two camps, one in favour of increasing the block size while the other preferring to leave it unchanged, which is often referred to as the 'scaling war'.

34 At present, there are two completely different proposals for a technical solution to increase capacity: increasing the block size and introducing second-layer transactions. The latter required the introduction of Segregated Witness (SegWit) in 2017, the preparation of which had also taken years. With SegWit, the block structure became 'more compact' (it was a kind of optimisation) by not recording every signature within a block. This, in turn, gives the green light to launching the Lightning Network, which would relieve the bitcoin network by making possible smaller transactions off the blockchain. More information about the SegWit and the Lightning Network: https://en.wikipedia.org/wiki/SegWit, https://en.wikipedia.org/wiki/Lightning_Network

In order for bitcoin to be used as money, it should fulfil the functions of money. It should be able to intermediate exchange and measure the value of goods (measure of value), facilitate the movement of goods and credit money (medium of exchange and payment instrument), and allow assets to be accumulated, i.e. function as a store of value.

High volatility of the price of bitcoin (see Figure 7) represents too high a market risk for the accumulation of bitcoin for transaction and investment purposes. Let us consider how a merchant could safely determine the price of its goods denominated in bitcoin if the exchange rate of bitcoin is able to move up or down by 5% to 15% per day against the world's number one key currency, the US dollar?

A currency is able to intermediate the exchange of goods only if its value is nearly constant and is widely accepted, because the relative prices of products are determined based on the value of the currency. An instrument that shows sudden price movements in both directions is able to fulfil this intermediary function only to a limited extent. Moreover, the acceptance of bitcoin by merchants as a payment instrument is quite limited. In 2017, the number of stores accepting bitcoin did not increase but actually continued to decrease. According to a study by James Faucette, an analyst of Morgan Stanley, of the top 500 online merchants, the number of players accepting bitcoin decreased from five to three from 2016 to 2017.[35]

It is a question to what extent this decrease is affected by the appreciation of bitcoin in 2017, which produced astronomical returns. If the use of bitcoin for transaction purposes remains marginal as a result of the continuously experienced positive effect on wealth, merchants will not be interested in introducing it as a new payment platform. In addition, it is worth mentioning in respect of the measure of value function that low-value purchases, such as paying for a coffee or soft drink with bitcoin, are excluded due to the increasing transaction fees. Since it would be absurd to assume that anyone would be willing to pay a transaction fee that is higher than the price of the product or service purchased.[36]

If money and merchandise are not able to change hands at the same time, the medium of exchange function is corrupted. In the case of bitcoin, protracted transfer times currently work against this function. If a consensus was reached between the parties on the capacity-increasing upgrades, which have been under preparation for years, and the protocol of bitcoin was developed, it would result in

35 https://www.bloomberg.com/news/articles/2017-07-12/bitcoin-acceptance-among-retailers-is-low-and-getting-lower

36 With respect to making payments in bitcoin, we must not forget the fact that – in contrast with purchases by debit and credit cards – the buyer pays the transaction fee.

a significant reduction in completion time (to 1 to 3 seconds)[37]. And all this would guarantee the consolidation of the medium of exchange function of bitcoin.

One of the forms of accumulation of wealth is setting aside money. The money must be suitable for being an instrument for hoarding (tesauration). For this, the permanent requirement of having a stable and non-decreasing value must be met. In recent years, the price of bitcoin denominated in US dollars had produced continuous growth up to December 2017 and showed parabolic growth in the last quarter of 2017, enticing an increasing number of new small and large investors to the market. For example, if someone had invested USD 1,000 in bitcoin in the summer of 2010 (which, at that time, would have been equivalent to placing a bet with that money on a horse in a race), they would have had a fortune of USD 242 million by the end of 2017 (see our note before Figure 8). Based on this, bitcoin apparently fulfils the store of value function, since its value has been continuously increasing, apart from periodic corrections, in recent years. However, bitcoin has shown significant depreciation against the main fiat currencies both in relative and absolute value since last December, strengthening bitcoin sceptics' opinions and questioning the sustainability of the previous increasing trend.

In the light of the above, we believe that at present bitcoin is not able to completely fulfil the functions of money. If the above-mentioned protocol-related developments were carried out and the tightness, depth and resilience of the market (market liquidity) of bitcoin further improved, we would see a possibility for bitcoin taking another step in the process of becoming money. In addition, of course, it would be necessary to reduce the volatility of its price, to which both the recently launched bitcoin futures markets and the continuously increasing market size contribute favourably.

3 BITCOIN: A NEW ASSET CLASS

Despite the fact that the market capitalisation of bitcoin has surpassed USD 200 billion recently, this peculiar virtual instrument is still surrounded today by confusion as to how it should be interpreted and classified. While the CFTC, the agency overseeing the US commodity futures market, considers bitcoin to be goods, the Internal Revenue Service (IRS) regards it as property. In certain cases, the US Securities and Exchange Commission (SEC) classifies it as securities, while the European Central Bank treats it as a convertible decentralised virtual currency.

37 The completion time of transactions on the currently tested Lightning Network is only a few seconds.

The term 'cryptocurrency' itself may be misleading to a certain degree because it suggests that cryptocurrencies form a subcategory of traditional currencies. In our opinion, in reality, we can talk about a completely new asset class. Consequently, it is more appropriate to use the term 'cryptoasset' for open, decentralised, virtual currencies based on cryptography.

Countless studies have been written on the distinction and categorisation of traditional asset classes. Of those, we would point out a paper by Robert Greer (1997), who drew a distinction between three superclasses of assets: capital assets, consumable/transformable assets and store of value assets (Table 1). The superclasses defined by Greer are based on the different fundamental economic features of assets and the correlation of asset returns.

Table 1
Categorisation of traditional asset classes by their superclass

	Capital assets	**Consumable/ transformable assets**	**Store of value assets**
	'Ongoing source of something of value … valued on the basis of net present value of its expected returns.'	*'You can consume it. You can transform it into another asset. It has economic value. But it does not yield an ongoing stream of value.'*	*'Cannot be consumed; nor can it generate income. Nevertheless, it has value; it is a store of value asset.'*
Equities	X		
Bonds	X		
Real estate	X		
Commodities		X	
Precious metals (gold)		X	X
Currency			X
Fine art			X

Source: Rober J. Greer (1997):'What is an Asset Class, Anyway?', *The Journal of Portfolio Management*

Based on Greer's findings, *Burniske* and *White* (2017) defined four main characteristics to distinguish between traditional asset classes: (1) investability, (2) politico-economic features, (3) correlation of returns: price independence and (4) risk-reward profile.

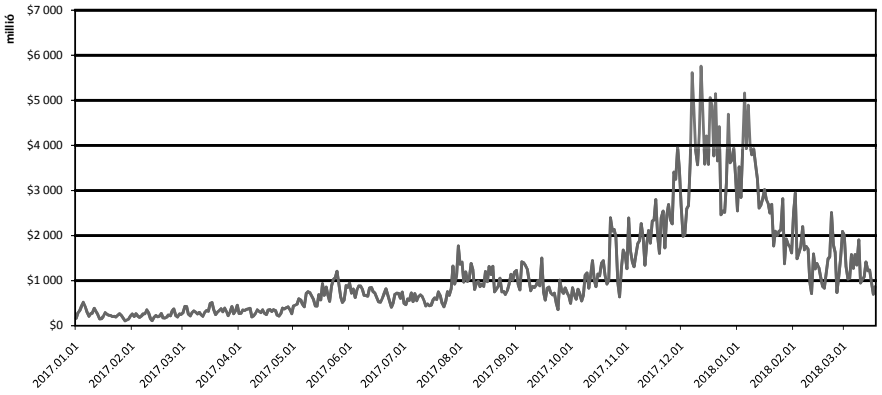
Investability was defined as a function of market liquidity. Second, in their opinion, the politico-economic profile of an asset is influenced by its intrinsic value, regulatory environment and utility. Third, price independence means the independence of the market value of an asset from the price of assets of another asset class, which they derive from the low correlation of returns on assets. Finally, they recommended to measure absolute returns and the volatility of asset prices to differentiate between risk-reward profiles.

For example, stocks (equities) and bonds can be included into different asset classes, because after they meet the condition of investability, they differ in the other three characteristics. While stocks embody receivables for an indefinite period, which is secured by the profit-generating capacity of a company in the future, bonds provide periodic payments only for a fixed period, which is secured by the asset value of the company concerned (politico-economic features). Furthermore, stock and bond prices move in an opposite direction in a low-risk macro-environment: if bond prices increase, stock prices will drop (price independence). A significant difference can also be found in risk-reward profiles, since stocks are essentially riskier instruments with higher returns, while bonds are less volatile investment assets which have a lower return-generating capacity.

Let us review the characteristics of bitcoin according to the above-mentioned four characteristics below.

The liquidity of the bitcoin market showed a significant increase in 2017. While transactions worth about USD 10 to 150 million were carried out between bitcoin and fiat currencies every day between 2014 and 2016, trading volume has gradually approached USD 4 billion from the second half of 2017 (Figure 6). Even if only the BTC-USD market is taken into account, which has the highest trading volume besides the BTC-JPY currency pair, the volume of transactions per day exceeds USD 1 billion. A market of such depth and liquidity is also suitable for conducting transactions amounting to even several hundred millions of US dollars without causing a significant swing in the price of bitcoin. In the light of the above, in our opinion, the previous criticism about the illiquidity and fragility of bitcoin does not hold. Consequently, the Bitcoin market meets the investability criterion.

Figure 6
Average daily bitcoin exchange trading volume in 2017, in USD million



Source: authors' elaboration based on data from https://blockchain.info

The speciality and uniqueness of bitcoin do not only lie in the fact that it does not have an intrinsic value. Its operational and regulatory system (governance) also differs significantly from those of other assets. Bitcoin operates in accordance with a protocol established through the consensus or agreement of a community. The protocol rules contain all information on the governance of bitcoin, the custody of deposits, the 'issue' and distribution of bitcoin, the transaction process and finally its audit, and is binding upon all players of the network. Any of these rules may be changed only and exclusively through the nearly full consensus of the Bitcoin community (otherwise the above-mentioned 'fork' occurs).

Although bitcoin may seem similar to traditional currencies or, for that matter, to gold in terms of its use and utility, its potential goes far beyond those. The operation of the Ethereum network is good evidence that blockchain-based cryptoassets can provide a number of different services other than mere data recording and settlement. Similarly to Ethereum, the Bitcoin protocol may function once even as a platform that automatically executes contracts, allowing Bitcoin to provide digital settlement services to a very wide group of assets from real estate and loans to Internet-connected-devices.

Based on the foregoing, we believe that Bitcoin is special also with respect to its politico-economic features, because there is no other asset class in the case of which the rules mentioned above would be concentrated to such a degree.

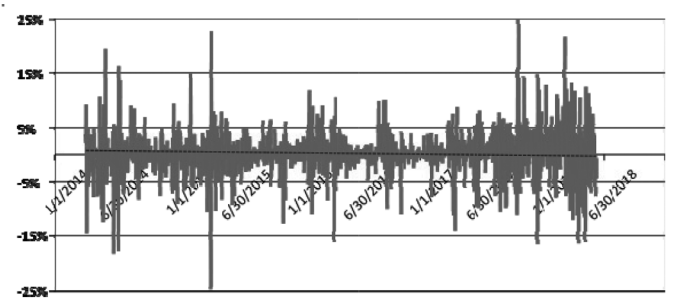
In the light of the differences shown above, the price of bitcoin is also expected to behave differently from that of the majority of classic asset classes. Correlation calculations are used the most often to measure and quantify the correlated movement of variables (in this case, bitcoin and other instruments) or the lack

of such movement. If the prices of two instruments show perfectly correlated movement, the correlation coefficient takes the value of +1, while in the event of perfectly opposite movement, the value of -1. In the latter case, when a portfolio comprises two instruments, the individual risks of the instruments can be perfectly eliminated. It follows from all this that in the case of a correlation coefficient of 0 or close to 0, the forces that affect the instrument prices are independent of each other. In our opinion, independence of such external economic effects is key to the uniqueness of bitcoin. Our assumption about the price independence of bitcoin set out in Section 4 of this paper is supported by fitting a dynamic conditional correlation (DCC-GARCH) model. Burniske et al. (2017) also obtained results similar to ours, who showed, using the rolling regression technique, that the price movements of bitcoin between 2011 and 2017 could remain independent of the prices of capital and commodities market instruments included in the study. Among other things, they concluded that bitcoin was the only asset that did not show any correlation or showed only minimum correlation with other asset classes.

Finally, the risk-reward profile of bitcoin is described below. While the risk level of an instrument is expressed by the volatility of its price, in respect of returns it is simply examined how the value of investment changes as a result of a change in its price over the reviewed time interval.

Although the indicators used the most often for quantifying volatility are standard deviation and variance, daily price changes also illustrate the fluctuation of instrument prices very well. It clearly transpires from Figure 7, which shows the changes in the daily closing price of bitcoin, that price changes over 10% are not rare on the bitcoin market. It occurred on 122 days from 1 January 2017 up until 11 March 2017 that the extent of price changes exceeded 5% and on 30 days it exceeded 10%. On the whole, average daily price change has been 3.8% in the period since 2017. Needless to say, a 3.8% change would be considered a major price swing, for example, in the case of the S&P500 stock market index. On the bitcoin market, however, it is literally considered an everyday movement.

Figure 7
Daily price changes of bitcoin



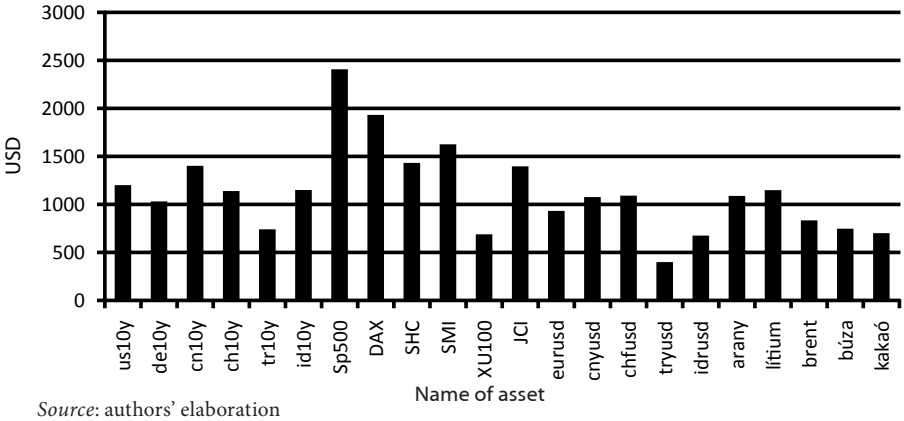
Note: based on BTC-USD closing prices at the Bitstamp exchange
Source: authors' elaboration based on data from https://www.quandl.com/

The broken line shows the average of daily price changes calculated with the one-week moving average method.

Figure 8 illustrates how much the value of a USD 1,000 investment made at the beginning of the sampling period (on 23 July 2010) would have changed if it had been invested in bitcoin or the other instruments reviewed. In the case of bitcoin, the final result is USD 242,702,012 if it had been closed on 8 December 2017. The results for the other investments are shown in Figure 8. It can be established that in the case of bond market instruments it is difficult to realise any return due to the near-zero interest-rate policy, while stock markets (except for the Turkish one) performed outstandingly. Meanwhile, no substantial profit was attainable in either foreign exchange or commodities. Therefore, due to the exponential increase in its price, a one-off extremely outstanding return could be achieved in bitcoin.

Figure 8

Value increase of an assumed investment of USD 1,000 between 23.07.2010 and 08.12.2017

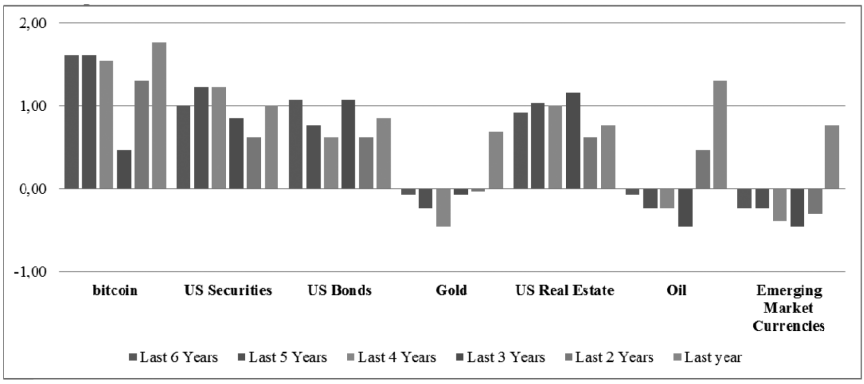


Source: authors' elaboration

As it follows from modern portfolio theory, neither asset price volatility nor the return-generating capacity of the instrument provides good guidance for making investment decisions. It is necessary to adjust the returns for volatility, i.e. risk. The indicator most often used in the literature for this purpose is the Sharp ratio, which defines the extra return on our investment in exchange for unit risk.

Burniske et al. (2017) calculated the Sharp ratios of bitcoin, US securities, US bonds, gold, US real estate, oil and emerging market currencies for several periods between 2011 and 2017. According to their results, bitcoin was the investment opportunity that promised by far the highest return over most timeframes (Figure 9).

Figure 9
Sharp ratios, 2011–2017



Source: Burniske C., White A. (2017): Bitcoin: Ringing the bell for a new asset class, Research White Paper, ARK Invest Research & Coinbase Inc.

In the knowledge of both the volatility of bitcoin and its absolute return-generating capacity, it can be stated that it has special features also in respect of its risk-reward profile.

In summary, the fact that bitcoin meets the condition of investability and it has different, unique characteristics in terms of politico-economic features, the correlated movement of prices and risk-reward profile confirms our assumption that bitcoin and other cryptoassets may not be included in the same category with the instruments of any already existing asset class. All this supports our proposition that a new asset class is emerging with the appearance of cryptoassets.

4 A COMPARATIVE ANALYSIS OF BITCOIN AND ASSETS OF OTHER CLASSES

4.1 Data and methodology

We compared the statistical properties of the end of the week rates of different money and capital market instruments[38] with the exchange rate of bitcoin against the US dollar (BTC/USD) between 23 July 2010 and 8 December 2017. The focus of our analysis was on the market of 10-year bonds (US10Y, DE10Y, CN10Y, CH10Y), leading stocks (S&P500, DAX, Shanghai Composite Index – SHC, Swiss Market Index – SMI), key currencies (EUR/USD, CNY/USD, CHF/USD) and commodities (oil, gold, lithium, wheat, cocoa).

We also included the exchange rates of more exotic instruments in our comparison, such as stock indices (XU100, Jakarta Composite Index – JCI), 10-year bonds and currencies of the Turkish and Indonesian market. As the volatility of bitcoin will be a significant aspect in our analysis, it was extended to the VIX index as well.

First, we compared descriptive statistics with their expected values for each time series by asset class, and then examined the volatility of the assets by selecting the most preferred model from the GARCH, GJR-GARCH, TARCH and APARCH models (1).

$$\text{GARCH: } \sigma_t^2 = \omega + \sum_{i=1}^{q} \alpha_i \varepsilon_{t-i}^2 + \sum_{i=1}^{p} \beta_i \sigma_{t-i}^2,$$

$$\text{TARCH: } \sigma_t = \omega + \sum_{i=1}^{p} \alpha_i |\varepsilon_{t-i}| + \sum_{i=1}^{o} \gamma_i S_{t-i}^{-} |\varepsilon_{t-i}| + \sum_{i=1}^{q} \beta_i \sigma_{t-i},$$

$$\text{GJR-GARCH: } \sigma_t^2 = \omega + \sum_{i=1}^{p} \alpha_i \varepsilon_{t-i}^2 + \sum_{i=1}^{o} \gamma_i S_{t-i}^{-} \varepsilon_{t-i}^2 + \sum_{i=1}^{q} \beta_i \sigma_{t-i}^2,$$

$$\text{APARCH: } \sigma_t^{\delta} = \omega + \sum_{i=1}^{p} \alpha_i (|\varepsilon_{t-i}| - \gamma_i \varepsilon_{t-i})^{\delta} + \sum_{j=1}^{q} \beta_j \sigma_{t-j}^{\delta} \quad (1)$$

Where σ_t stands for conditional volatility, ε_{t-i}^2 for normally distributed random error representing innovations or shocks and S_{t-i}^{-} for the dummy variable denoting the asymmetry caused by negative error term. For the purpose of model selection, we were looking for the minimum Bayesian information criterion (BIC) among models with a homoscedastic outcome based on *Cappiello* et al. (2006). Finally, we fitted a dynamic conditional correlation model (DCC-GARCH) to the sample (2) to assess correlations with bitcoin.

$$\sigma_{it}^2 = \omega_i + \sum_{p=1}^{P_i} \alpha_{ip} e_{it-p}^2 + \sum_{q=1}^{Q_i} \beta_{iq} \sigma_{it-q}^2, \quad (2)$$

We used the MFE and USCD toolboxes developed by Kevin Sheppard of the Matlab 2014a software for the necessary calculations and model fitting.

38 Source of the data: http://stooq.com

4.2 Results

Ideally, money and capital market instruments should show asymmetry and a kurtosis of around 3 at an expected value of 0, assuming normal distribution, zero autocorrelation, homoscedasticity and stationarity (*Kiss*, 2017). In practice, these expectations are typically met in the case of logarithmic differentiation only in respect of expected value and stationarity (Table 2). It is observable that, except for cocoa and EUR/USD, none of the assets follow a normal distribution (*Jarque–Bera* $p > 0.05$), while the returns of German and Swiss 10-year bonds, the Swiss Market Index, the Swiss franc and the Indonesian rupiah show extreme skewness (a fat-tail). In addition, autocorrelation and heteroscedasticity also appear in many cases.

We can conclude that there are no descriptive statistics which are typical to a specific asset class but not to others (Swiss-based assets are an exception). Cocoa approximates our ideal expectations the most closely and fulfils all the criteria. Bitcoin, by contrast, is also characterised by asymmetry, a fat tail, non-normal distribution and autocorrelation.

Table 2
Descriptive statistics for the different assets

Asset		Moments				Normal distribution	Autocorrelation	Heteroscedasticity	Unit root
		mean	standard deviation	skewness	kurtosis	Jarque-B p	Lung-B p	Arch-LM p	ADF p
Bonds	us10y	0.00	0.05	0.40	3.77	0.00	0.02	0.04	0.00
	de10y	-0.01	0.44	-0.26	35.96	0.00	0.00	0.11	0.00
	cn10y	0.00	0.02	-0.01	4.47	0.00	0.78	0.86	0.00
	ch10y	-0.01	0.41	-1.48	20.47	0.00	0.00	0.33	0.00
	tr10y	0.00	0.03	0.70	7.35	0.00	0.10	0.32	0.00
	id10y	0.00	0.03	0.14	4.50	0.00	0.25	0.33	0.00
Stocks	S&P 500	0.00	0.02	-0.41	5.29	0.00	0.16	0.36	0.00
	DAX	0.00	0.03	-0.60	5.50	0.00	0.45	0.62	0.00
	SHC	0.00	0.03	-0.76	6.82	0.00	0.06	0.37	0.00
	SMI	0.00	0.02	-1.46	10.50	0.00	0.32	0.35	0.00
	XU100	0.00	0.03	-0.60	4.45	0.00	0.31	0.41	0.00
	JCI	0.00	0.02	-0.47	6.81	0.00	0.03	0.18	0.00

Asset		Moments				Normal distribution	Autocorrelation	Heteroscedasticity	Unit root
		mean	standard deviation	skewness	kurtosis	Jarque-B p	Lung-B p	Arch-LM p	ADF p
Foreign exchange (USD)	BTC	0.03	0.16	0.89	8.09	0.00	0.00	0.07	0.00
	EUR	0.00	0.01	-0.21	3.43	0.06	0.84	0.86	0.00
	CNY	0.00	0.01	-0.55	6.65	0.00	0.00	0.00	0.00
	CHF	0.00	0.02	1.79	30.70	0.00	0.07	0.16	0.00
	TRY	0.00	0.02	0.04	3.73	0.02	0.45	0.53	0.00
	IDR	0.00	0.01	0.42	13.82	0.00	0.07	0.08	0.00
Commodities	gold	0.00	0.02	-0.43	4.18	0.00	0.18	0.16	0.00
	lithium	0.00	0.03	-0.58	5.87	0.00	0.18	0.24	0.00
	Brent	0.00	0.04	-0.24	4.86	0.00	0.20	0.33	0.00
	wheat	0.00	0.04	0.42	4.36	0.00	0.16	0.23	0.00
	cocoa	0.00	0.03	0.02	3.22	0.71	0.26	0.29	0.00
	VIX	0.00	0.15	0.54	5.72	0.00	0.00	0.00	0.00

Source: authors' calculation with MFE toolbox

As a next step, we examined based on the Bayesian information criterion (BIC) in accordance with Cappiello et al. (2006) which models of the GARCH family and with which *p*, *o*, *q* delay values can be fitted to the time series with a homoscedastic outcome (Table 3). In this case, there are obvious differences between the asset classes: the most complex APARCH model is needed for 10-year bonds and Swiss-based assets may only be described by asymmetric GARCH models. By contrast, for commodities, the simplest GARCH(1,1) model is sufficient to describe a process in which volatility in the previous week account for 90% of prices in the current week. It were asymmetric TARCH(1,1,1) models that could be fitted to assets on the stock and foreign exchange markets, where typically weakened exchanged rates resulted in higher volatility. German and Swiss bonds represent a special case. Here, increasing returns led to higher volatility. A similar result was obtained for the Swiss franc and bitcoin among currencies: strengthening exchange rates went hand in hand with higher volatility.

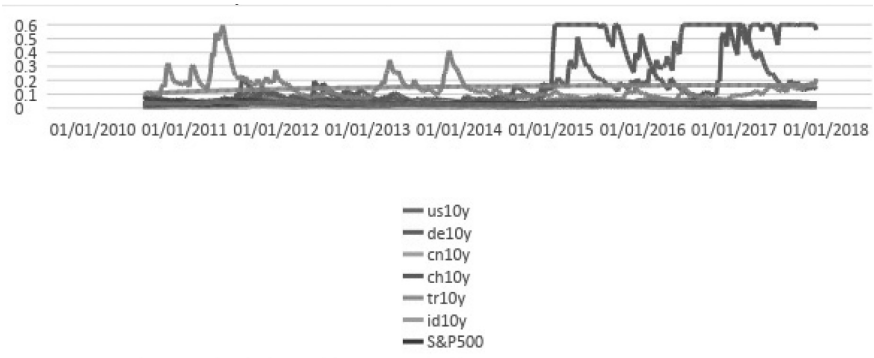
Table 3
Volatility model parameters

Asset	**us10y**	**de10y**	**cn10y**	**ch10y**	**tr10y**	**id10y**
constant	0.00	0.00	0.00	0.00	0.00	0.00
alpha	0.00	0.13	0.13	0.08	0.12	0.17
gamma	0.11	-1.00		-1.00		
beta	0.95	0.84	0.60	0.75	0.83	0.76
nu		1.60		2.81		
Model	TARCH (1,1,1)	APARCH (1,1,1)	GARCH (1,1)	APARCH (1,1,1)	GARCH (1,1)	GARCH (1,1)
Asset	S&P500	DAX	SHC	SMI	XU100	JCI
constant	0.00	0.00	0.00	0.00	0.00	0.00
alpha	0.00	0.00	0.14	0.00	0.19	0.09
gamma	0.24	0.18		0.14		0.26
beta	0.83	0.86	0.86	0.84	0.11	0.66
nu						
Model	TARCH (1,1,1)	TARCH (1,1,1)	GARCH (1,1)	TARCH (1,1,1)	GARCH (1,1)	TARCH (1,1,1)
Asset	bitusd	eurusd	cnyusd	chfusd	tryusd	idrusd
constant	0.01	0.00	0.00	0.01	0.00	0.00
alpha	0.28	0.07	0.13	0.15	0.00	0.00
gamma	-0.18		0.00	-0.60	0.09	0.30
beta	0.81	0.92	0.83	0.84	0.90	0.84
nu				0.30		
Model	TARCH (1,1,1)	GARCH (1,1)	TARCH (1,1,1)	APARCH (1,1,1)	TARCH (1,1,1)	TARCH (1,1,1)
Asset	gold	lithium	Brent	wheat	cocoa	VIX
constant	0.00	0.00	0.00	0.00	0.00	0.00
alpha	0.06	0.08	0.09	0.04	0.05	0.00
gamma						
beta	0.87	0.87	0.90	0.93	0.93	0.99
nu						
Model	GARCH (1,1)	GARCH(1,1)	GARCH (1,1)	GARCH (1,1)	GARCH (1,1)	GARCH (1,1)

Source: authors' calculation with UCSD toolbox

After the first months of 2015, German and Swiss bond returns had pronounced conditional volatility (Figure 10). Apart from this, volatility well above the market average was recorded only for bitcoin.

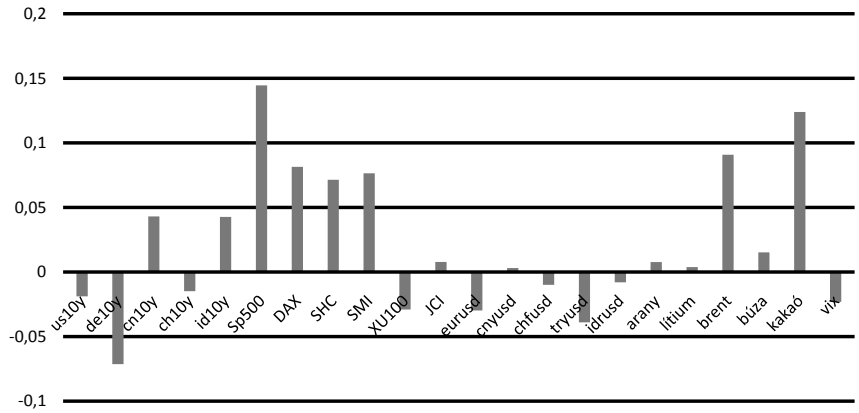
Figure 10
Conditional volatility values



Source: authors' calculation with UCSD toolbox

Traditionally, the literature points to a lack of correlation between bitcoin and other assets. This seems to be a valid statement based on average dynamic conditional correlation values (Figure 11).

Figure 11
Average dynamic conditional correlation (DCC-GARCH) values

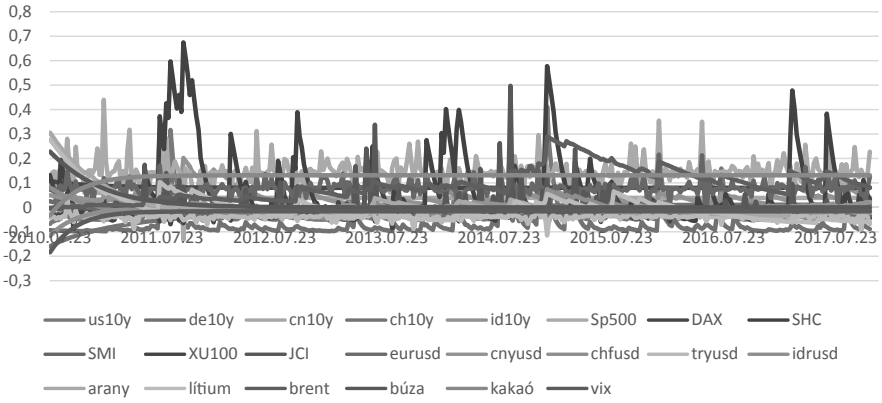


Source: authors' calculation with UCSD toolbox

However, examining correlation over time, obvious cases of moderate correlation with either the Chinese, the S&P500 or the Indonesian stock market index are observable over short periods in the past (Figure 12).

Figure 12

Dynamic conditional correlation (DCC-GARCH) values



Source: authors' calculation with UCSD toolbox

5 IN PLACE OF A SUMMARY

We are now living in the last years of the second decade of the 21st century, the age of digitalisation and big data, when we may control even our coffee machine and soon practically any of our household appliances remotely, contact by electronic means between clients and traditional service providers from banks and bodies of public administration to educational institutions becomes increasingly widespread, and we use different cloud-based services and social media platforms to digitalise and share with each other a significant portion of our private lives. In our increasingly digitalised society, the concept of a new kind of money cloaked in IT codes was inevitable to appear.

Even though many of us may not be aware, it is a fact that the grim and painful consequences of the global financial and economic crisis of 2007–2009 and the bailout packages put together to protect an irresponsible and insufficiently regulated banking system have marked a turning point in the world of digital currencies. Although digital currencies had been around even before the crisis, as a common feature, they all involved a central counterparty.

The revolutionary feature of Satoshi Nakamoto's proposal was to leave out this central authority. What he actually did was combining technologies that had already existed in previous decades in an innovative way. The concept of the distributed and decentralised database, which is at the heart of the blockchain technology, is essentially based on the working principles of the peer-to-peer (P2P) network, public key infrastructure (PKI) encryption and cryptographic hashing.[39]

Satoshi's brainchild Bitcoin was the first cryptoasset to initiate actual change in settlement systems as we knew them. Although at present, the emergence of cryptocurrencies does not yet pose an actual challenge for banks, with time, as the technology becomes more widely adopted and the issues encountered are tackled as it leaves its infancy, the cryptocurrency asset class will be a key player in the world of finance.

The extremely fast-paced growth witnessed on the cryptocurrency market[40], in terms of both the number of instruments and soaring prices, and their subsequent sharp decline as well as the impact of all this on the financial system impel financial market participants and regulators to have a closer look at the functioning of this novel market. Institutions who choose to ignore the spread of this technology risk being sidelined in the long term.

Cryptocurrencies as a new asset class are no doubt in an early stage of life. Therefore, we believe that it is not too late for any of our readers to get to know the potential of the blockchain technology and to tap it while they can. We are of the opinion that the innovative distributed ledger technology[41] and the infrastructure and processes it encompasses may bring increased simplification and efficiency into the financial world, and in combination with existing technologies pave the way for a new generation of financial services. Of course, this will not be the end of the road, as the possibilities offered by the innovative blockchain technology may bring about fundamental changes in a number of fields, including the insurance market, land registries or the health sector.

As a conclusion to our paper, let us cite the words of Nobel-prize winner Keynesian economist Paul Krugman, originally published in the journal *The Red Herring* in

39 The first widely-known P2P network was implemented by the file sharing service of Napster, launched in June 1999. The PKI technology has been used since the 1990s. It allows for secure transactions between two untrusted parties, e.g. by timestamping transactions, a feature that was first introduced as part of this technology. (We are all familiar with the simplest PKI implementations. One of these is SSL encryption.) Finally, cryptographic hashes (e.g. ECC or Elliptic Curve Cryptography) have been used for authentication since 1985, however, they came into more widespread use only around the turn of the century, among others, in designing security solutions for mobile phones.

40 At present, more than 1,500 cryptoassets are recorded.

41 'Distributed ledger technology' is a synonym of 'blockchain technology'.

1998: 'By 2005 or so, it will become clear that the Internet's impact on the economy has been no greater than the fax machine's.'[42]

Krugman was obviously quite wrong to make such a premature statement. We are of the view that the blockchain technology of our times will be as great an opportunity and challenge for the future as was the appearance of the Internet in the 1990s. Our advice for all of us is therefore to be on our guard.

REFERENCES

Burniske C. – White A. (2017): Bitcoin: Rising the bell for a new asset class. *Research White Paper*, ARK Invest Research & Coinbase Inc.

Cappiello, L. – Engle, R. F. – Sheppard, K. (2006): Asymmetric Dynamics in the Correlations of Global Equity and Bond Returns. *Journal of Financial Econometrics* 4, 537–572. o., CoinDesk: State of Blockchain 2018, 2017-Q4 Report, http://ww.coindesk.com.

Cointelegraph (2018): Exponential Growth: Cryptocurrency Exchanges Are Adding 100,000+ Users Per Day, 2018.01.07, https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day.

Hackett, R. – Wieczner, J. (2017): How High Can Bitcoin's Price Go in 2018? *Fortune*, 2017.12.21, http://fortune.com/2017/12/21/bitcoin-price-value-prediction-bubble/.

Fodor D. – Speiser F. (2014): *Automotive embedded systems* [Autóipari beágyazott rendszerek]. TÁMOP-4.1.2.A/1-11/1-2011-0042, Veszprém, Pannon Egyetem.

Greer, R. J. (1997): What is an Asset Class, Anyway? *Journal of Portfolio Management* 23, 86–91., http://dx.doi.org/10.3905/jpm.23.2.86.

Kiss, G. D. (2017): *Volatility, extreme fluctuations and capital market contagion* [Volatilitás, extrém elmozdulások és tőkepiaci fertőzések]. Szeged, JATEPress.

Trubetskoy, G. (2017): Electricity Cost of 1 Bitcoin (Sep 2017)., https://grisha.org/blog/2017/09/28/electricity-cost-of-1-bitcoin/.

The Telegraph (2017): Bitcoin mania: Google's top searches in 2017 dominated by digital currency craze. 2017.12.13, http://www.telegraph.co.uk/technology/2017/12/13/bitcoin-mania-googles-top-searches-2017-dominated-digital-currency.

42 http://www.digitaljournal.com/article/346996