# David Biczok - Master's Thesis:

# THE FUTURE OF BITCOIN AND THE BLOCKCHAIN TECHNOLOGY

Thesis Supervisor: Roger H. Hartmann


**Student ID:**

0160677836

1. August 2018, Luxembourg

# Table of content

# Chapter 1. - Abstract

My research question for the Masters Thesis is the following: The future of bitcoin and the blockchain technology.

Bitcoin and blockchain are one of the latest technologies, that had a huge impact on the banking industry, and therefore it is a hot topic in the media too. Since they are such new technologies, they are far from being in their maturity, which means it is not clear yet, if they will fundamentally change the way we think about banking in general, or they will be only the next bubble like the Dotcom Bubble was in early 2000s. With my thesis my aim is to collect all the relevant information about these new technologies, organize the knowledge in a way, that I will be able to highlight their advantages and disadvantages next to their impact on the banking industry and vice versa. As a second step I will summarize the data with the purpose of being able to draw possible trends about the outcome of the bitcoin usage to see, if it is really a useful alternative payment method with real added value, or just an investment instrument which had extraordinary returns in 2017. With the collected information I also intend to forecast how the blockchain technology will have a possible impact on the bank sector, and what new possibilities it could bring into our lives in the next few years.

# Chapter 2. - Introduction

I am coming from the Online Payments / eCommerce / IT sector, where I have been active for the last 9-10 years, and FinTech has always been one of the fields, which was really interesting for me.

I started my career back in Budapest, Hungary at an online payment service provider (PSP), where I participated in setting up the company from scratch, and as such I have seen several aspects of this industry. With my first employer I gained extensive knowledge about Fraud Prevention, Risk Management, Project Management, Finance and Industry Standards, which lead to the second half of my career with my current employer. Since I work in Luxembourg, I am responsible for all the payment related activities of a public listed eCommerce Group, meaning that I need to be up to date with all the latest trends in the online payments and fintech world.

On one hand this was one of the reasons, why I decided to submit my application for the Banking and Finance programme at the University of Luxembourg. My motivation was to widen and deepen my knowledge about industry trends, best practices and corporate governance.

Regarding Bitcoin and the Blockchain technology: on the other hand I am directly impacted by this new payment method / investment instrument (depending on the end user), as I am also experimenting with it by implementing it into the websites of the Group I am working for.

Since it is a brand new payment method, which is different from the traditional ones like wire transfer, credit card, mobile payments, etc. I thought it would have been useful to dig deeper into the technology and reveal its possible future and risks to know, where it will end up. It has direct impact on the performance of my employer by being a bitcoin and alternative coin acceptor, therefore I am curious to see, if it has the potential to reinterpret industry standards across the whole sector.

Going back to my career: since I have seen the online payments industry both from the perspective of the merchant and the service provider, I am able to provide input for my research both from the perspective of the bitcoin / blockchain user and acceptor. My intention is not only trying to predict the future about online payments and banking, but also to create a detailed manual about the blockchain technology itself, that can work as a handbook for anyone, who wants to know more about why it was created, what it is exactly, and how it has already changed the payment industry.

Bitcoin is in the centre of attention lately, and everybody talks about how its price skyrocketed in the end of 2017, but I am sure, that only a small proportion of people would know exactly, how it works, why it was created and what problem it intended to provide a solution for. The ground of my hypothesis is, that I have been following bitcoin and blockchain in the last few years, and my experience was, that there were only a few educational articles and videos online, that are clear enough to make it easily understandable for the general public. Lately the situation has improved a bit, since bitcoin became a hot topic in the second half of last year (2017), but I believe, that there is a need for comprehensive studies about the possibilities it can bring in the next few years to be prepared for the risks the technology involves.

This is basically, what I would like to support with my thesis: I would like to create an easily understandable manual about the technology, that highlights its advantages and risks involved, next to explaining the coming changes in the banking industry (PSD2), that together with the blockchain technology can fundamentally change the way we are used to banking today.

# Chapter 3. - Literature review

This is the most interesting part of my study: a technology that is created in the middle of the digitalization era, consequently based on the existence of internet and all the related information is stored in the cloud, the best source of information is also the internet itself, therefore the most comprehensive literature on the topic is “google”.

But to avoid relying completely on the internet, and to obtain much more accurate research results, my strategy for the study will encompass three big group of information sources as follows:

1. **Online literature:** there are plenty of articles, interviews and videos about the bitcoin and the blockchain technology online, so for the first part of the thesis, where I compile and provide a handbook about the system, I will rely on these sources. Since these articles are publicly accessible, I will compare various standpoints of different people to collide their opinions on the topic and to reveal particular aspects of the blockchain. I plan also to use Hungarian articles in the research, as bitcoin and bitcoin mining are also well known in Hungary and there are several online forums dealing with the specific know-hows. These sources will provide me enough information to establish the basis of the thesis and to introduce the next chapter, where I will investigate the risks of the blockchain technology.

   Finding the proper knowledge base about the risks requires a deeper research, as it is already a much more precise field compared to general information, but still manageable with online literature. I will pay attention strictly, that risk is a subjective topic, as each people on the Earth bears a different amount of risk appetite. My findings on this chapter will also help to elaborate, what the major risks of bitcoin and the blockchain technology are and, if there is any other industry specific risk involved too.

2. **Own experiences:** by the time I finish the Thesis, I will have around two months of comprehensive data from a bitcoin acceptor viewpoint, since I am testing it as a payment method on the websites operated by my employer. I will use this information to compare it to other online payment methods like credit card payments, bank transfer, mobile payments and other country specific alternative payment methods like iDeal in the Netherlands, Bancontact Mister Cash in Belgium or Sofortüberweisung (lately called as Klarna) in Germany. My aim is to see how bitcoin is performing compared to traditional ways of transferring money, and how likely people are choosing it over other payment methods. I intend to use this data to decide what bitcoin is exactly: and alternative payment method, that provides several advantages to the user, or an investment instrument used for speculative activities. I have been monitoring my professional network for feedbacks about this question, and for the time being I tend to think, that it is more of an investment instrument (excluding the fact that its price was on the top in the end of 2017).

3. **European acquiring banks and bitcoin processors:** luckily due to my current position, I have an extensive network of payment service providers, acquiring banks and bitcoin processors, whom I have already started to interview about the upcoming PSD2 changes. I believe the new legal framework will stir up the current status in the banking industry allowing non-bank players to access bank account information. In my eyes this might launch a wave of high level of innovation, such as it happened in 1986 after the deregulation in the bank sector. For this reason I devoted one chapter to explain PSD2 in details and to investigate the potential impact on cryptocurrencies and the blockchain technology. I have also collected information from a European PISP (Payment Information Service Provider), who developed a system excluding third parties from the payment flow without any blockchain related logic used, which might be an interesting alternative to cryptos. I would like to demonstrate their

solution in the thesis as a smart extension of the current system.

I will involve bitcoin processors in the research too, whom I will ask about protective steps they did to keep their positions on the market, because if their services remain as it is today, they might lose competitiveness on the long run. The first signs are already there: I constantly visit payment related forums and I obtained two big differences in 2018 compared to 2017: this year booths of bitcoin processors have appeared on payment conferences, which shows the interest in the technology. But on the other hand, traditional payment service providers started to offer their bitcoin processing solutions as a part of their services.

Combining these three perspectives; my own experiences, input of European banks and online literature, I will be able to provide a detailed summary about the current status of bitcoin and the blockchain technology, and an unique forecast about potential outcomes, shifts or changes in the bank sector, that already takes into consideration the innovative activities of new players appearing on the market after the introduction of the PSD2 directive.

# Chapter 4. - Work plan and methodology

My guide in the research will be Roger H. Hartmann, who has an extensive experience of 35 years in the bank sector, therefore his knowledge can be a huge added value for the thesis. We had our kickoff meeting on 22. February 2018 about the topic and we setup the roadmap, when I will deliver which part of the research. The work plan for writing the thesis will be the following:

1. I have prepared the Thesis Proposal the same week, when we had the kickoff meeting with the Professor (19-25. February) and I sent it over to him for a review;

2. The week after (1st week of March) I have received input from the Professor, that the the Thesis Proposal is fine as it is and it was submitted to the University for approval;

3. I have received the approval from the University on the week starting with the 5th March, so I could have started writing the Thesis;

4. I will write the Thesis in the following 4-8 weeks (5. March - 30. April). The Professor will be three times in Luxembourg during these weeks, so in case it is needed, we will meet for a catch up to receive extra input for the research.

5. I believe the work will be in final status by the end of April 2018, and I will be able to submit it for grading to the University of Luxembourg.

The chapters of the study are the following:

- The history of the blockchain and bitcoin

    - Popularity and usage of the technology
    - The hype around bitcoin in the end of 2017
    - Alternative coins (Ethereum, Litecoin, Dash, Ripple) and market capitalization
    - Is it an investment instrument or an alternative payment method?
    - Explaining the blockchain technology in details

- Risks of the blockchain technology
    - Is it a problem to be unregulated? Possibilities for manipulation?
        - The “50% +1” rule and the role of Mining Pools
        - ICOs and liquidity risk
    - Environmental impacts and the power needs of Bitcoin Mining
        - Is it a sustainable way of doing business?
    - Explaining the sources of volatility of the bitcoin
        - Do big hedge funds invest in bitcoin?
    - Security risks of the blockchain technology (including historical examples)
        - Does it really provide anonymity for the user?
        - Lost bitcoins
        - AML and Terrorism funding involving the technology

- Introduction of the PSD2 regulation
    - History of the Payment Service Directive
    - Innovation brought with the PSD2: the appearance of PISPs and AISPs
        - Closed loop platforms created by PISPs and AISPs
    - Interactions between the blockchain technology and the innovative technologies created by the PSD2

- Conclusion: will the bitcoin and the blockchain survive?

# Chapter 5. - The history of the blockchain and bitcoin

In 2017 one of the mostly trending words was Bitcoin, and people, who are not exactly sure what it is or how it works, started using it in their everyday life. The reason is simple: up to 2009 money could have only been issued by the following three bodies: **central banks** through printing money, by **credit institutes** through creating money via loans, or by **e-money licensed institutions** through electronic money issuance. The common point in all cases was, that money issuance was done within an extremely regulated framework. Even today the banking industry is the most regulated sector on Earth since it fulfils a double role: it gives loans to borrowers and collects outstanding monies simultaneously. But this has changed in January 2009, when the first bitcoin has been mined within an unregulated and decentralized environment. Bitcoin was the first cryptocurrency invented in **2008** by Satoshi Nakamoto (as he calls himself, but his true identity is still a question up to this day) together with the blockchain technology.[1]

[1] Egri Szilvia, 5 Jan. 2018, “Bevezető a Kriptovaluták És a Blockchain Titokzatos Világába, https://fintechzone.hu/bevezeto-kriptovalutak-es-blockchain-titokzatos-vilagaba/

We use the word cryptocurrencies for all digital forms of payment, which are issued by a network of computers (peer-to-peer: P2P network) after solving complex mathematical equations, instead of being created by the traditional licensed bodies within a regulated environment. These mathematical equations are named as cryptography, which were called to life after the Second World War, since there was a need for secured communication channels for obvious reasons. Currently more, than 1000 cryptocurrencies exist, and bitcoin is the best known of all of them.[2]

The backbone of bitcoin is the **blockchain technology**, which is basically an encrypted database of transactions (ledger), shared among all participants of a public network and therefore also verified by the users. The difference between the existing system and what blockchain brought us is, that it does not require over-regulated third party entities like banks to maintain several ledgers in parallel but only one, therefore its IT requirement is also lower, and all participants of the network can have access to it anytime. As a consequence a much stricter control is applied on it, leaving less opportunities for data manipulation. It does not require dedicated infrastructure to keep the system running, but instead the users of the network are themselves the infrastructure. It means, that no external entities need to be involved in the flow of transactions, but the network itself fulfils all the necessary functions for the same services, that was only available with fully specialised institutions in the past. This new technology has tons of advantages for their users, which I have collected in the next chapter.

## 5.1 - Popularity and usage of the technology

The popularity of the blockchain derives from its peculiarities brought to the finance sector. Maintaining only one joint database might sound not that interesting or unique idea, but its advantages make it really competitive against the traditional banking services:

- **Lower costs:** since the transactions are running through a shared and public network, it does not require a dedicated IT infrastructure by a central entity, therefore its cost of processing and maintenance fees are also limited. Basically anyone can be a member of the blockchain network with a computer. Then it is up to the preferences of the user when and how much capacity he or she is willing to allocate for mining purposes (mining = solving mathematical calculations to encrypt information). The motivation behind is simple: the miner, a person, who designates computing capacities for encrypting transaction details, that are later stored in the common ledger, or better known as the blockchain, receives bitcoins as a payment for their computing services. As a result the overall transaction costs are also waived.

- **Lower risk of fraud and higher security:** since the database of transactions (ledger) is shared among all the participants of the network, no third party providers (like banks) are involved in the flow of processing transactions, leaving less space for fraudulent activities. It's difficult, but not impossible to alter the ledger, since it is

[2] Cara McGoogan and Matthew Field, 8 March 2018, "What is cryptocurrency, how does it work and why do we use it?" https://www.telegraph.co.uk/technology/0/cryptocurrency/

certified by all the members of the network and it is only approved, if it matches by 51% of the users. The ledger stands from blocks, which are basically batches of encrypted transactions with all their details combined. These blocks are stored after each other in chronological order, and to be able to add a new block to the chain (this is where the name blockchain originates from) its encrypted hash has to be the same for at least 51% of the miners. The below picture summarizes the above:

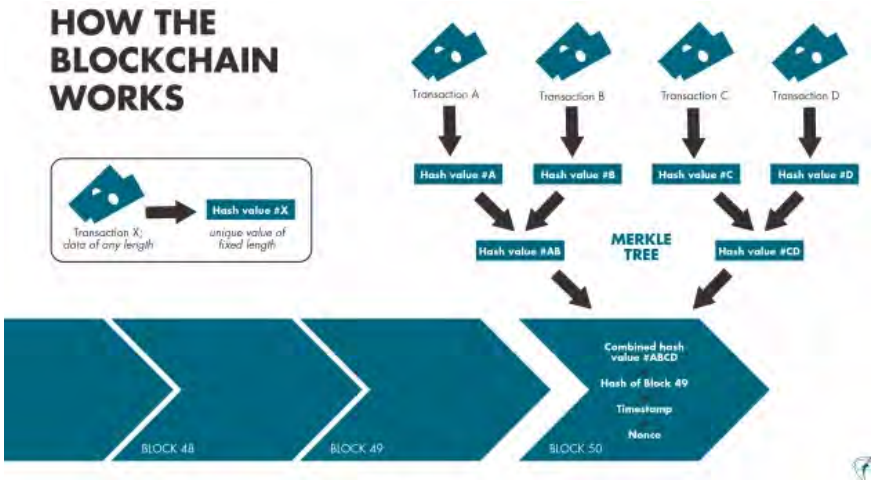



Image source[3]: https://www.heise.de/tp/features/Blockchain-Die-Technik-die-nicht-vergessen-kann-3986173.html

- **It provides anonymity:** there is a general belief about bitcoin, that their users can initiate their transaction in a fully anonym environment, but this is only half of the truth. Indeed all the transactions and their details are encrypted, and with the current computing capacities it would take years to decode it, but still the ledger is there and publicly available and shared among all participants. Also quantum computers might be a threat for the blockchain as they might be able to decrypt the blocks much faster. To increase complexity the system does not transfer bitcoins from one sender to one receiver, but it combines several transactions of several senders, and forwards them to several receivers, which makes it even more difficult to track in case of decryption. It is also true, that instead of names or personal details the system uses generated addresses for the users, but in case someone is able to connect these addresses to identities of people, then all of their payments, should it be sent or received, can be traced back since the backlog of transaction is publicly accessible for anyone.[4]

- **Increased accuracy:** since the blocks of transactions in the database are recorded for good and they are certified by the members in the network, whose consensus of 51% or more is needed to approve a new block, therefore the chances of inaccuracy is significantly lower. Of course this does not guarantee 100% accuracy, because the garbage-in garbage-out theory is still applicable for the blockchain technology too, and it might open theoretical doors for manipulation, but it also means, that the settlements risk is lower too, and the transactions reach their beneficiaries with much

[3] Christoph Jehle, 10 March 2018 “Blockchain: Die Technik, die nicht vergessen kann”, https://www.heise.de/tp/features/Blockchain-Die-Technik-die-nicht-vergessen-kann-3986173.html
[4] Jordan Tuwiner, 2015, “Is bitcoin anonymous?” https://www.buybitcoinworldwide.com/anonymity/

higher chances, than before.

- **Decentralized:** this might be one of the most important peculiarities of the blockchain technology as the system itself relies on a peer-to-peer network of users, and not only on specific financial institutions as we have it within the traditional banking framework. It is basically saying, that there is a monetary system that provides global coverage for their products and services and still there is no such thing as "Bitcoin Bank", that could go bankrupt. The crisis of 2008 highlighted how fragile the centralized banking system is, and that some trigger events can launch domino effects, which can push banks into insolvency. One of the main advantages of being decentralized is, that it eliminates liquidity and credit risk, and reduces systemic risk.

- **Speed:** of course there are also solutions for payments in the traditional banking world, that take only seconds to be processed, like the SEPA Instant Credit Transfer network, but it has its limitations. In case today we would like to initiate an international transfer from one bank to another, it might take several days to reach its beneficiary. If we look behind the curtains, we can easily identify the major obstacles with the current setup: centralised bank system with several intermediary banks slowing down the flow of money, who process only few batches of transactions every x hours and does not operate on public holidays, etc. With the blockchain network we can basically initiate an instant payment to anyone across the globe, since the clearing of the block of transactions are running non-stop 24/7.[5]

Now we see, that Bitcoin might be an answer for several weaknesses of the traditional banksystem, but to have such a unique network today the technology had a long way to go through including many difficulties to cope with and it is still not over:

There were several attempts in the past to create encrypted databases of transactions, but Bitcoin was the first one, that finally was launched. The best known attempts were between 1998 and 2008, namely Bit Gold and B-Money, whose theoretical backgrounds were published in the corresponding media, but their developments required to go live were never completed. In contrast, after the announcement of Bitcoin in **2008**, it became publicly available for anyone, who wanted to participate in the network, and bitcoin mining could have officially started in **2009**. Bitcoin mining is the official term for computing processes required for encrypting batches (or blocks) of transactions. It is basically solving complex mathematical algorithms, where the miner receives Bitcoin as a reward. The first block ever encrypted is called as the "Genesis Block".[6]

The first recorded payment with Bitcoins was done on **22. May 2010** or better known the "Bitcoin Pizza Day", when Laszlo Hanyecz, an early Bitcoin user paid 10.000 BTC for two pizzas, which would have cost him around $25. This was an important day in the history of blockchain, because up to this point bitcoin was only mined and not traded, and basically no

[5] European Payments Council AISBL, 2017 "SEPA Instant Credit Transfer" https://www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer
[6] Everest Group, 11 May 2016, "Defining Blockchain", https://www.everestgrp.com/2016-05-blockchain-technology-bfsi-benefits-market-insights-20805.html/

monetary value was assigned to a cryptocurrency before. The irony of fate is, that in case Laszlo would have kept his bitcoins, they would worth around $100 Million as of today.[7]

As usually it used to happen after pairing value to something, it opened several opportunities and bitcoin started to attract more and more people into the world of cryptocurrencies. Of course, the number of users were still limited around that time, but day by day more and more bitcoins started to exchange owners and the number was increasing significantly. As a consequence and also proving, that there was an increasing demand for cryptocurrencies and business potential in the technology, newly established bitcoin-competitors started to appear on the crypto market. By **2011**, so two years after the launch of bitcoin the first altcoin (alternative coins) startups were already operating: namely Namecoin and Litecoin.

An increasing network based on secured and anonym currencies were not only an interesting opportunity for alternative coin providers, but became an attractive mean of payment for criminal activities, tax evasions and money laundry as well. Of course these news have reflected shadow over the reputation of bitcoin and we did not need to wait too long till it gained the attention of financial regulators.[8] The first step against the blockchain technology was committed by the State of California, when it issued a cease to the Bitcoin Foundation, a non-profit organization founded in **2012** with the aim of promoting the technology. Their concern regarding the activity of the organisation was, that in their eyes the Foundation was actively participating in money transmitting, which requires a license, but obviously the organisation did not have any, therefore it was violating the Financial Code of California.[9]

**2013** was another milestone in the price of the Bitcoin and for the emerging market of cryptocurrencies. The growing popularity of cryptos especially in **China**, but also among the Silk Road users (online marketplace ran on the untraceable Tor Network, where people could have bought illegal drugs) combined with the idea of a decentralized and secured currency significantly increased bitcoin demand and also its value, and it has reached $1000 for the first time. At that time the number of bitcoin users were still limited, which left open doors for market manipulation. There is one well known research titled “Price Manipulation in the Bitcoin Ecosystem”, that summarizes all the suspicious elements and concludes, that this peak in 2013 might have been caused by one person only. Most probably this was also the reason of the decline, that started shortly after and resulted in the bitcoin price bottoming at $300. It took another three years till it reached $1000 again.[10]

---

[7] Rob Price, 28 November 2017, “Someone in 2010 bought 2 pizzas with 10,000 bitcoins - which today would be worth $100 million”
http://uk.businessinsider.com/bitcoin-pizza-10000-100-million-2017-11?r=UK&IR=T

[8] Bernard Marr, 6 December 2017, “A short history of bitcoin and crypto currency everyone should read”, https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/2/#1150a7d0533c

[9] Jon Matonis, 23 June 2013, “Bitcoin Foundation receives cease and desist order from California”, https://www.forbes.com/sites/jonmatonis/2013/06/23/bitcoin-foundation-receives-cease-and-desist-order-from-california/#30d7d939518c

[10] Neil Gandal, JT Hamrick, Tyler Moore, Tali Oberman, 2017, “Price manipulation in the bitcoin ecosystem”
http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_21.pdf


Image source[11]: http://www.bitcoin2040.com/bitcoin-price-history/

Between **2014** and **2015** series of scams and criminal cases connected to cryptocurrencies came to light. Just to mention a few: one of the biggest scandals were the Mt. Gox case, where 850,000 bitcoins in value of $450M have disappeared from one day to another from the bitcoin wallets of its clients. It is still not clear what exactly happened, but the signs refer to hackers having the money stolen. To show the importance of the case and the risks of centralization, Mt. Gox was once one of the world's largest exchange platform and intermediary for cryptocurrencies, based in Japan and handling 70% of the bitcoin transactions worldwide, but after these events they went immediately bankrupt.[12] Also during these years Silk Road founder Ross Ulbricht, who was arrested in 2013 found guilty for money laundering, computer hacking and drug trafficking.[13]

Next to the scandals the expanding demand for bitcoin was unstoppable, and to follow the trend, well known merchants started to implement bitcoin as a payment method on their websites. Since 2014 people were able to make payments on Microsoft's websites for downloading Windows or Xbox games, computer producer Dell also offered bitcoin payments on their webpages, and software developer Zynga has also introduced it for purchases in their applications. By the end of 2015 approximately 160.000 merchants were offering cryptocurrencies as a mean of payment on their websites.[14]

[11] Bitcoin 2040, 30 September 2017, "A historical look at the price of bitcoin", http://www.bitcoin2040.com/bitcoin-price-history/
[12] Jake Adelstein, Nathalie-Kyoto Stucky, 19 May 2016, "Behind the biggest bitcoin heist in history: inside the implosion of Mt. Gox", https://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox
[13] Nate Raymond, 5 February 2015, "Accused Silk Road operator convicted on U.S. drug charges", https://www.reuters.com/article/us-usa-bitcoin-trial/accused-silk-road-operator-convicted-on-u-s-drug-charges-idUSKBN0L82H920150205
[14] Bitcoin-made-easy, 2018, "About Bitcoin" https://bitcoin-made-easy.com/about-bitcoin/?ccce=cart&a=add&domain=register&PageSpeed=noscript

After the sharp improvement of global bitcoin acceptance the opinion of the general public also started to transform slowly, and cryptocurrencies were not directly associated with illegal transactions on the dark web anymore. This new perspective helped to provide ground for one of the most important researches about the topic, which was done in **2016** by Paolo Tasca, Shaowen Liu and Adam S. Hayes, who discovered, that the technology is not focusing on supporting "sin" industries like illegal drugs, gambling, money laundry anymore, but there have been a shift in the composition of usage. The status review was necessary after the dualities of the previous years: series of scandals combined with increasing usage and acceptance, bitcoin being offered as a payment method by brands like Microsoft, Dell or Uber or recognizing it as a real currency in Japan, that has similar characteristics as everyday money. The paper played a really important role to form the opinion of people about cryptocurrencies in a positive direction.[15]

Also in 2016 with the arrival of the alternative coin, Ethereum, which is the biggest competitor of bitcoin today, ICOs were introduced to the crypto world. ICO stands for **Initial Coin Offerings**[16], which is basically a fundraising technique outside of the tradicional banksystem. It is an alternative to IPOs, where instead of shares of newly listed firms, tokens or coins of projects can be purchased in exchange for bitcoin or ethereum during a given period of time. It was a groundbreaking way for collecting money for new companies or projects.[17]

## 5.2 - The hype about bitcoin in the end of 2017

**2017** and especially the last quarter of the year was the period, when bitcoin got really into the centre of attention. To interpret it in numbers: since bitcoin was launched in 2009 it was trading mainly below $1000, except in 2013 when it peaked for a short period of time a little bit above a thousand dollars, but most probably due to price manipulation. But knowing the events in the end of 2017 we can call its first 8 years pretty "stable". Even in the beginning of 2017 its price was below $1000 (1. January 2017: 1BTC = $967.93), and it did not change significantly till April - May  neither. However the second semester of the year brought some surprises: from the summer of 2017 bitcoin has started its rally and skyrocketed in the coming months, and finally it set its all time record on **17. December at $19783.06**:

[15] Paolo Tasca, Shaowen Liu , Adam S. Hayes, 1 July 2016, "The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment relationships", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762
[16] Nathaniel Popper, 27 October 2017, "An explanation of the initial coin offerings", https://www.nytimes.com/2017/10/27/technology/what-is-an-initial-coin-offering.html
[17] Antonio Madeira, 28 February 2018, "How does an ICO work", https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/

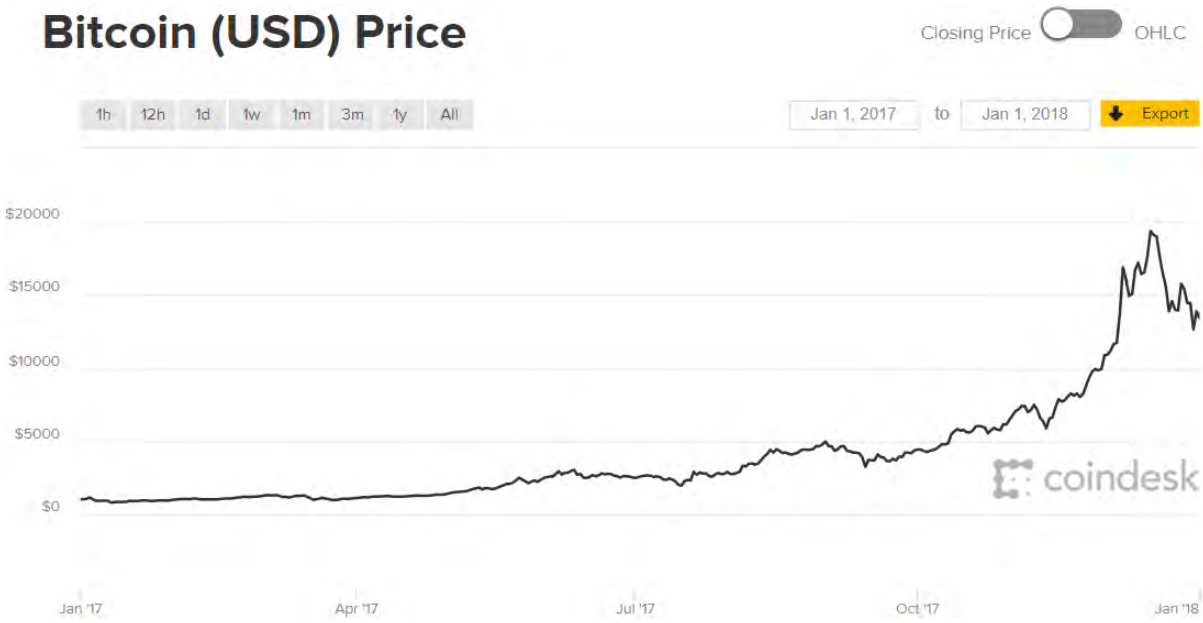



Image source[18]: https://www.coindesk.com/price/

To find the reasons behind this chart, we need to investigate the major events in the world of cryptocurrencies and narrow it down to the ones, that might have had the biggest impact on the price. As in the years before, 2017 was no different either; more and more websites are now offering bitcoin as a payment method, people are getting to know about it since the media is also dealing with cryptocurrencies on a recurring basis, regulators and financial institutions are getting more acceptable with the blockchain technology: Japan accepted it as a legitimate currency, Russia announced the development of a Cryptorubel and more and more Japanese and South Korean investors invest their money into cryptos. Several payment service providers and acquiring banks are adding bitcoin to their portfolio, and ICO is still a thing, that generates additional demand for cryptocurrencies. Of course with the increasing usage of bitcoin fraud increased in parallel, therefore 2017 was not free of scandals neither. As a reaction in September 2017, the Central Bank of China (also because of China being the World's largest bitcoin producing country) saw the risks involved in cryptocurrencies and therefore issued a ban on the blockchain technology. Luckily for the bitcoin owners it did not have significant impact on the price.[19]

All the above explains the constant upwarding slope of the price chart, but not the peak in the end of the year. In my opinion the rally that led to the almost $20000 bitcoin price and multiplied its market capitalisation of $15Billion almost ten times should be a combination of the following three fundamental innovations:

- **Investment funds** adding bitcoins and cryptocurrencies to their portfolio: after the media started to deal with cryptocurrencies and as a consequence, the existence of an alternative investment product, that can generate outstanding returns in a very short period of time reached the general public, the demand for bitcoins were

[18] Coindesk, 2018, "Bitcoin (USD) Price", https://www.coindesk.com/price/
[19] Sara Hsu, 15 January 2018, "China's shutdown of bitcoin miners isn't just about electricity", https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-shutdown-of-bitcoin-miners-isnt-just-about-electricity/#728df844369b

increasing heavily. From one side people were putting pressure on institutional investors like hedge funds to offer it in their portfolio, on the other hand them recognizing the business opportunity it might include, they started to buy bitcoins up in a bulk, that helped to drive up the price. Additionally a new breed of hedge funds started to appear, who were specialized only in cryptocurrencies. Just under one year in 2017 the number of such funds increased **from 30 to 130**, which meant a huge potential of new money coming in. The downside of these changes were, that such a centralization in the group of bitcoin owners can bring some unnecessary but additional risks into the picture: in case a hedge fund decides from one day to another to cash out their money invested in cryptocurrencies, it would result in a big drop in the price.[20] This is exactly what started to happen **between 18. December 2017 and 5. February 2018**, when Mt.Gox, the company who got hacked in 2014 while, that time they were handling 70% of the overall bitcoin market capitalization, sold $400Million worth of Bitcoins in 5 stages (according to their public statement it was done to indemnify their customers for their losses suffered in 2014). Compared to the current market capitalization, it might have been not the main reason why the price dropped a record amount of **$2300 in two days** on 7. March 2018 (from $10600 to $8300), but according to their statements they still own $1.7 Billion worth of cryptos, which they are planning to sell. As it is a bit bigger portion of the overall wealth invested in bitcoins, **it might have further negative impacts on the investors in the coming years**.[21]

- **Bitcoin Futures Contracts**: by 2017 several traditional investors and investment funds did not invest in cryptocurrencies yet, since their opinion about the technology was, that it has no intrinsic value, and where for example gold has a real commodity behind, bitcoin was “just” traded in an unregulated and decentralised environment backed with basically nothing. But this viewpoint has changed in December 2017, when the Chicago Mercantile Exchange (CME) introduced futures contracts on bitcoins, and from that point investors could speculate on the price movements without actually holding the bitcoins themselves. Additionally this opened a new spectrum for institutional investors too attracting more and more money coming in and boosting the price up, because with the futures contracts they received a tool in their hands to hedge against potential drops in the price of bitcoins.[22]

- **Bitcoin ETFs**: Exchange Traded Funds, that offer bitcoin in their portfolio have been attempted to be approved in the past (2013) by the Winklevoss brothers. Their name might be familiar from the history of Facebook, as they have sued Mark Zuckerberg for claiming the idea of the social network to be theirs before Zuckerberg actually created the website. That time they could have not won the trial, but they were

[20] Nathaniel Popper, 6 November 2017, “Hedge funds push up the price of bitcoin to new highs”, https://www.nytimes.com/2017/11/06/technology/bitcoin-hedge-funds.html?rref=collection%2Fbyline%2Fnathaniel-popper
[21] Chuck Jones, 12 March 2018, “Blaming Mt. Gox For Bitcoin's Recent Price Drop Just Doesn't Compute”, https://www.forbes.com/sites/chuckjones/2018/03/12/blaming-mt-gox-for-bitcoins-recent-price-drop-just-doesnt-compute/#600e2ee17d61
[22] Jackie Wattles, 10 December 2017, “Bitcoin jumps after futures trading begins”, http://money.cnn.com/2017/12/10/technology/bitcoin-futures-trading/index.html

compensated outside of the court. When the facebook case was settled, they have already seen the potential in the blockchain technology, so they used the wealth they received after the lawsuit and they invested into startups dealing with cryptos, and purchased 1% of the outstanding bitcoin stocks. Their vision was to lift cryptos to the level of mainstream funds, but to do so, they needed the approval of the Securities and Exchange Commission.[23] Around that time the S.E.C. had a strongly negative opinion about turning a fund, that contains certain cryptocurrencies in their setup, publicly available for everybody, as they are traded in an unregulated environment, they were extremely volatile and often used for illegal activities. All together the idea was rejected. As an answer, the Winklevoss brothers created a fully regulated cryptocurrency exchange (Gemini.com), where the users could acquire, sell or exchange cryptocurrencies the same way as on any other stock exchanges, and on top they launched their first bitcoin ETF on it. Later in the first semester of 2017 due to the increasing media activity dealing with cryptos and additional pressure from people, the S.E.C. decided to review their decision about denying bitcoin ETFs. Unfortunately they rejected them this time too.[24] The final breakthrough was brought by the introduction of futures, options and swaps in the bitcoin world: two ETFs (ProShares Bitcoin ETF and the ProShares Short Bitcoin ETF), that had cryptocurrency futures in their portfolio were allowed by the S.E.C. and the NYSE to be publicly traded and to let investors to bet on the price movements of the bitcoin.[25]

Bitcoin had an outstanding year in 2017: regulators were getting more acceptable with it, the media was full of the cryptocurrency hype, derivative instruments were created around them, and with their help ETFs were able offer them in their portfolio, even only in an indirect way yet. Proving the potential in the technology the two best performing ETFs in 2017 were sharing the same OTC bitcoin tracking security (Bitcoin Investment Trust). Both ARK Web x.0 ETF (ARKW) and ARK Innovation ETF (ARKK) reached extremely good returns, close to almost 100% under one year.[26]

### 5.3 - Alternative coins (Ethereum, Litecoin, Dash, Ripple) and their market capitalization

The original blockchain technology has brought several new aspects into how we think about money today, but since it is a new way of “banking”, which has not matured yet, it still includes several weaknesses, or development opportunities. The technology with the media attention together has created ground for alternative coins to be invented and to provide answers or solutions for additional features or security gaps. Currently more than a thousand alternative coin types exist and 18 of them have already a larger funding volume than $1

[23] Portfolio.hu, 5 December 2017,“Itt vannak a világ első bitcoinmilliárdosai”, https://www.portfolio.hu/vallalatok/itt-vannak-a-vilag-elso-bitcoinmilliardosai.270067.html
[24] Allan Eberhart, 6 April 2017, “SEC Rejects Bitcoin ETFs: Should You Reject Bitcoin Investments?”, https://www.forbes.com/sites/allaneberhart/2017/04/06/sec-rejects-bitcoin-etfs-should-you-reject-bitcoin-investments/#6228f25379bd
[25] Thomas Franck, 20 December 2017, “NYSE files to list bitcoin ETFs, bringing cryptocurrency a step closer to mainstream”, https://www.cnbc.com/2017/12/20/nyse-files-to-list-bitcoin-etfs-bringing-cryptocurrency-a-step-closer-to-mainstream.html
[26] Sumit Roy, 21 December 2017, “Top performing ETFs of the year”, http://www.etf.com/sections/features-and-news/top-performing-etfs-year

Billion. In this chapter I will present the biggest competitors of bitcoin from market capitalization point of view and I will explain, what problem they were planned to provide a solution for:

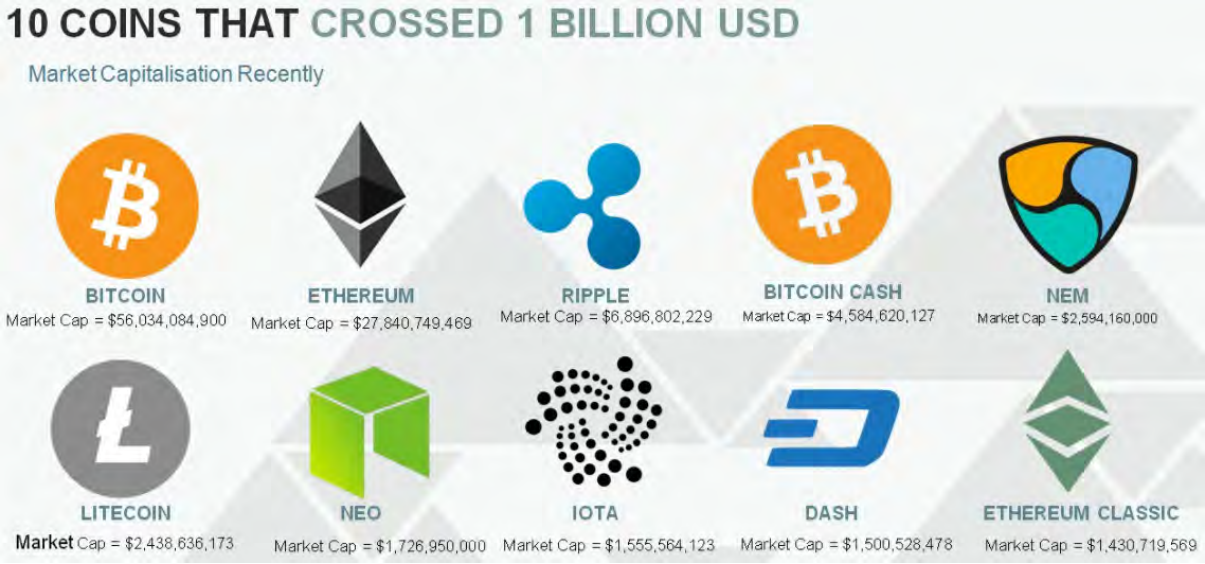



Image source[27]: https://rilcoinblog.com/2017/09/08/10-coins-that-crossed-1-billion-usd/

**Bitcoin and bitcoin cash**: At this point we all know, that bitcoin was the first cryptocurrency, that was ever launched, and it has the most users and market capitalization as of today, but in 2009 when it went live, there were some limitations written in its code to prevent future abuses. One of these limitations was the size of a block: originally it was 1 Mbyte, which was set to protect the network from overcharging through spamming or ddos attacks and leaving it unusable for real users. Most probably even the creator of the blockchain did not expect such popularity for the technology, as already in 2015 a block included 600 Kbytes of data. This meant, that 60% of the capacity of the blockchain has already been used up, and in case it would have increased above 1 Mbyte, users should have waited much longer transaction processing times, making the network less competitive against traditional means of payment. **Bitcoin Cash was introduced on 1. August 2017** with the intention to solve this issue. It has not replaced the classical bitcoin, as even among the existing users were no consensus about the legitimacy of its existence: one part of the people thought that bitcoin should have been left unchanged, since this is the key for a real secure system, but the other part supported an upgraded version. As a consequence on 1. August the common ledger of bitcoin was split into two and left separated for the future: one was for bitcoin classic and another fork for bitcoin cash. The main changes in bitcoin cash were its increased block size (from 1 Mbyte to 8 Mbyte), which enabled the processing of eight times more transactions under the same amount of time, and also the setup of a block, which has been adjusted in a way, that it could store more data. With these improvements the processing capacities of the blockchain technology have increased to the level of PayPal or VISA, but for the price of multiplying its IT requirements. For this reason only those miners could have the possibility to mine it, whose IT infrastructure was much advanced, than the average users'. These changes got also criticised as they have opened new possibilities for

[27] Rilcoinblog, 8 September 2017, "10 Coins that crossed 1 Billion USD", https://rilcoinblog.com/2017/09/08/10-coins-that-crossed-1-billion-usd/

51% attacks by being one step closer to centralization. But even with such factors bitcoin cash was able to attract a substantial market capitalization of **$15 Billion** by the beginning of 2018.[28]

**Ethereum and Ethereum Classic**: we call ethereum the platform on which ether is being traded. It was initially launched on 30. July 2015 with the aim of taking the blockchain technology to the next level. The basic characteristics of ether are similar to bitcoin, as it is processed also in a decentralized environment, mined in the same way as bitcoin, but instead of providing only a channel for transferring money from a sender to a receiver, its platform was much more advanced, than that. The biggest difference is in the possibility of creating so called **smart contracts**, which are basically applications that run on the ethereum platform without any downtime, and can do pre-configured actions triggered by specific events. For example we can create a contract, where we order an amount to be transferred to someone else in the event of a given trigger. Basically the invention of the ethereum platform became the ground for programming **crypto-options**, and **derivative contracts**. Showing the potential and the possibilities it opened, it has attracted a market capitalization of $50 Billion for ethereum and $1,5 Billion for ethereum classic (as of 18. March 2018) less than in three years. The difference between the two coin types is, that the original blockchain was manually changed for one of them, after the system was hacked (the DAO hack) in 2016, resulting in a $50 Million loss for ether owners. One part of the ethereum community supported the idea to hold the stolen money and to compensate their original owners, but another part of the users was on the viewpoint that the blockchain must be kept untouched after its initial launch. Since no consensus was reached in the question, both types of ethereum were kept.[29]

**Ripple**: the goal of this cryptocurrency is pretty simple: it aims to create a global settlement network, that converts and transfers money from anywhere around the World within 4 second maximum. The startup was launched in **2012** and it claimed to be the best alternative for the SWIFT and the Western Union networks next to much less costs. For this reason more and more banks have already accepted ripple as a new platform of **transferring money**, and even Western Union is experiencing with it, how to add its features to their services. As of today it has gained almost **$24 Billion** and by doing so, it became the 3rd largest alternative coin by market capitalization.[30]

**Litecoin**: It is one of the first alternative coins, which is available on the market since 7. October 2011, and brought only minor improvements to the blockchain technology. Its main characteristics are the same as bitcoin's, but litecoin provides a bit faster processing (2.5 minutes per block, instead of 10 minutes as for classical bitcoin), improved security and higher coin limits. These minor developments were still enough to attract more, than $8 Billion invested into this alternative coin.[31]

[28] Admiral Markets, 2018, "Mi a Bitcoin Cash?", https://admiralmarkets.hu/education/articles/trading-instruments/mi-a-bitcoin-cash
[29] Unknown author, 8 February 2018, "What is Ethereum", https://www.finder.com/ethereum
[30] Unknown author, 8 February 2018, "What is Ripple", https://www.finder.com/ripple
[31] Unknown author, 8 February 2018, "What is Litecoin", https://www.finder.com/litecoin

**Neo**: it is the blockchain developed by China as an answer to the creation of ethereum. It was officially launched in August 2014, and on one side it had similar characteristics to ethereum like supporting smart contracts, but on the other side, it had some quite unique features. The main difference between ethereum and neo is, that on the neo network there is not only one cryptocurrency processed, traded and mined but two: Neo and Gas. Neo is like a share of a company and it represents stakes in the future of the neo blockchain. It cannot be divided into smaller fractions, which is possible with bitcoins. There is a chance, that it might be an issue in the future to buy neo tokens, in case the price increases, but there are techniques for cryptocurrencies, how to split the more expensive ones into smaller pieces. Gas is like a dividend of a company, that you receive after holding neos. Since its launch its market capitalisation has already reached $4 Billion.[32]

Next to the ones mentioned above, there are further eleven cryptocurrencies, that at the moment have more than $1 Billion invested in them: Cardano, IOTA, Stellar, EOS, Dash, Monero, Tether, NEM, TRON, VeChain, Lisk. Their characteristics are more or less similar to bigger cryptos, with some minor differences and goals for each.

## 5.4 - Is it an investment instrument or an alternative payment method?

For the time being I was focusing mainly on the advantages of the blockchain technology, that is indeed a groundbreaking innovation with several exclusive features, that the traditional banking system does not support, but now I would like to talk more about the practical side of using bitcoin as a payment method. By the time of writing this Thesis, I will have collected 3-4 weeks data from a bitcoin and alternative coins acceptor point of view, therefore this chapter will reflect my personal experiences and opinion on the usability. Seeing the results, I will explain why I think, that the blockchain technology is only a good start of something bigger, but not an effective and matured payment method yet:

If we check, how bitcoin works today, we can consider it a simple “bank transfer” and nothing else. But even from bank transfer point of view, it is not really user friendly. To mention a few disadvantages: it is a bit complex and however the internet is full of articles about the blockchain, there are not so many easily understandable manuals out there, that clearly explains, where to start from, if we want to begin paying with it. First we need to open a **bitcoin wallet**, which is basically the equivalent of any other e-wallet on the market, but it supports cryptocurrencies. Once it is done, we need to fund that wallet somehow. The average user most probably will not start mining cryptos, but they will buy their bitcoins through an online card payment or a simple bank transfer. Basically I have just highlighted the first two problems with the technology regarding its user experience. We added several extra steps in the checkout process, with which we increased the complexity of a flow, that in the end has the same result as before: initiating an online payment transaction and to exchange our money for some goods or services on the internet. All eCommerce merchants agree on the fact, that the checkout process is one of the most important parts of the whole user experience. Therefore it must be seamless from the beginning to the end, with the least

[32] Unknown author, 8 February 2018, “What is Neo”, https://www.finder.com/neo

steps involved till the final payment is finished, because we will lose potential customers with each extra barrier and we kill our conversion rate quickly.

Secondly: in case someone funds his or her bitcoin wallet through a simple card payment, or a bank transfer, the anonymity, why someone has chosen using this method is partially lost. In case someone can assign identities to cryptocurrency transactions, then the whole transaction history of the user can be traced back, since the ledger is shared among each member of the blockchain network, meaning it is publicly accessible for anyone.

Also, if someone wants to protect his or her identity on a higher level, then there are several other payment methods already available on the market, that are much easier to use. Prepaid cards, or e-vouchers for example like Neosurf or Paysafecard just to name a few do the work pretty well and they are not even target of the current wave of fraud, as it points mainly to cryptocurrencies lately. But there are also several mobile billing, premium sms or voice call payment methods, that provides anonymity for the customer and it even excludes the step of purchasing a prepaid card or voucher. However these methods have their limitations in maximum chargeable amounts, number of transactions per customer, or supported industries. Additionally, they are pretty expensive for the merchant compared to other payment solutions, since the mobile network operators take a large proportion of the payment amount as fees. As a result the group of merchants, that provides mobile or telephone payment methods are limited, but depending on the industry of the business, it can be a really powerful tool for taking the money.

Finally, one of the biggest weaknesses of bitcoin is customer protection. Since there is no supervisory board or institution guarding the blockchain, like we have the card schemes as VISA or MasterCard for card payments, there is no guarantee for getting our money back in case someone misuses our bitcoin wallet. After creating the whole system in an unregulated environment, we cannot expect to have a custodian or overseeing body, who could provide compensation for our losses. Therefore **for the average user it is safer to use card payments**, because the well organised dispute handling protocols, the chargeback processes of any major card brand all over the world, will protect their cardholders to advance online payments in general. In the world of card payments the whole system was created in a way, that also the merchant should be held responsible, and therefore interested in protecting the card details of its customers. In case merchants do not comply with the different rules in place, they are risking serious fines from the card schemes:

- There are general regulations, which are applicable for all merchants providing card payments: the most important set of rules is the PCI DSS regulation created by the major card schemes (Visa, MasterCard, Discover and American Express).

- The acquiring banks, who provide merchant accounts for payment processing, have also strict sets of rules about business models, KYC, AML regulations, website requirement, that protects the cardholder in case he or she buys something from the merchant.

- On top of the PCI DSS and the acquiring banks' requirements, there are different limits applied on the total accepted disputed, and fraudulent transaction levels of the seller, that must be kept below the thresholds during the whole lifetime of the merchant account. To avoid penalties or risking to have the merchant account used for payment processing to be closed, merchant must comply with all sets of rules above.

In case someone prefers bank transfers instead card payments for any reason (for example he or she does not like to provide his or her card details on websites, as they think it's not safe enough), there is a way for initiating wire transfers through the direct debit platform. In this case the customer authorizes his or her bank to allow money to be pulled out of his or her bank account in exchange for services or goods he or she intends to buy. But even this method is there for a long time, therefore it had its time to mature as much as in several countries it could have become the leading payment method. iDeal in the Netherlands, Bancontact Mister Cash in Belgium, ELV in Germany, Przelewy24 in Poland just to name a few are basically simple wire transfers from one bank account to another with an advanced infrastructure built around the system.

Regarding the conversion rate: I am monitoring the success rate of bitcoin and alternative coin transactions initiated and successfully finished, and the result is around 1 successful transaction out of every 100 attempts, or in other words: 1%. Obviously there are many customers, who are just discovering the payment flow out of curiosity, since bitcoin is a hot topic lately, but this approval rate is still very low. On the other hand credit card approval rates can be as high as 80-85% depending on the transaction types and amounts (initial transaction, subscription based, etc.). As for the number of transactions via cryptocurrencies: on well established websites with millions of visitors a day, where credit card and other traditional payment methods generate thousands of successful transactions on a daily basis, I can count the successful bitcoin transactions on one hand of mine.

Finally my thoughts about the preference penetration among bitcoin and any other alternative coins: I have mentioned, that there are more, than a thousand different cryptocurrencies on the market these days, and there are 18 of them, that has a market capitalisation over $1 Billion, but the truth is, that people are using these cryptos mainly as an investment instrument, and not really to pay with them. Since I have been monitoring the performance of crypto transactions, 100% of the successful payments were initiated by bitcoin, and zero with any other alternative coins like ethereum, litecoin or neo.

It is a bit contradictory, that reports from the end of 2017 about cryptocurrency usage have already mentioned, that people have initiated 52.3% of all crypto transactions through ethereum, and 33% only via bitcoins, where newer researches from 2018 show, that ripple started to outperform even ethereum. But the truth is, that these transactions are not generated by buying goods online, but people are investing into them and trading among each other with speculative intentions as the price volatiles.[33]

[33] Trustnodes, 22 November 2017, "Ethereum now handles more transactions than all digital currencies combined", https://www.trustnodes.com/2017/11/22/ethereum-now-handles-transactions-digital-currencies-combined

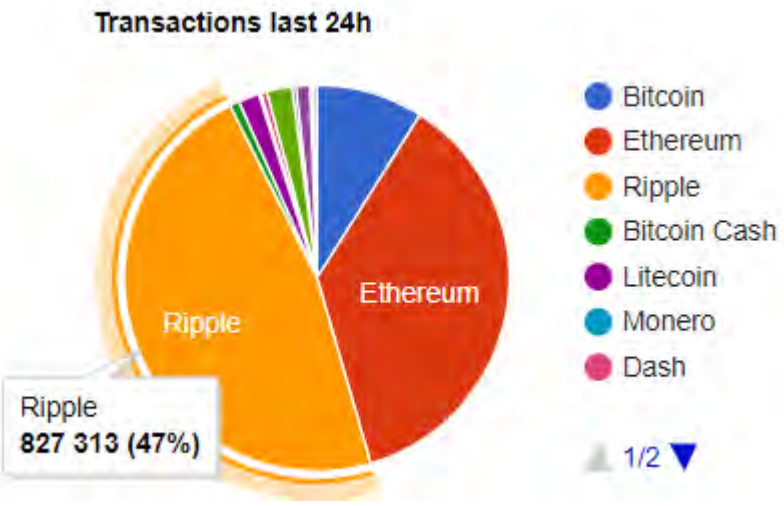



Image source[34]: https://bitinfocharts.com/cryptocurrency-charts.html

## 5.5 - Explaining the blockchain technology in details

The following chapter will be a bit technical oriented, but it is necessary to understand the background, why the blockchain was created and for what problem it intended to provide a solution to be able to point out the risks and threats these kind of platforms contain.

In the past, if someone gave money to another person, it was not really difficult to trust each other, that the money will reach the beneficiary, since the movement of amounts were direct: from one hand to another, without any extra participants involved. This has changed with the innovations brought by the boom in telecommunication, which were implemented also by the bank sector almost immediately. The new communication networks banks have setup among each other allowed people to transfer money from one side of the world to the other, without the need of the sender physically meeting the receiver. The only problem with this flow was the involvement of third parties: banks. Trust in each other of persons to exchange money relied and depended completely on external parties, without having any control over what these outsiders were doing. Just to mention a few risks: what, if we make an order to the bank to initiate a transfer, but the order is not taken into the ledger, because someone from the bank has simply forgotten to do it? Or what, if the order was created, but the bank made a mistake and sent a different amount, or to a different bank account? What, if someone from the bank did these “mistakes” on purpose? And we have been transferring money in this framework since Western Union has set up the first telegraph network in 1872 and created the basics of the traditional wire transfer infrastructure. The logic behind the process has remained more or less the same for more, than a decade up to 2008, when bitcoin was invented. So the first question the blockchain technology was searching an answer for was, how we can maintain 100% trust between sender and receiver, if all the time when we do a wire transfer, we have to rely completely on someone else. The obvious solution was to

[34] Bitinfocharts, 18 March 2018, “Cryptocurrency charts”, https://bitinfocharts.com/cryptocurrency-charts.html

exclude all the third parties like banks from the flow, which became the main goal of the crypto network. But the exclusion of banks has introduced another problem, because someone still had to do their most important job: maintaining the ledger, what includes the details of our transfers. This is where the groundbreaking innovation of the blockchain technology comes into picture:

Let's imagine, that there is a group of people, who agrees, that they do not want to involve banks when they transfer money among each other, but it is fine for them to share their bank account details with the participants (without revealing their true identity behind the bank accounts to remain more or less anonym). The smallest number of people in the group should be 3 (eg.: David, Adam and Tia). As a start we give everyone pens, paper sheets and envelopes, and we ask them to write on the sheets the transfers done in the group (one sheet per participant). For example, if David wants to give 10€ to Adam, he has to say out loudly, that he will send 10€ to Adam, so Tia also hears it. First everyone has to check, that David has at least 10€ on his account, and in case he has, all of them write on his or her paper, that David transferred 10€ to Adam. They keep on writing the transactions till they reach the end of their sheets and they have three copies of the same list of transactions. Now they have to put them in their envelopes so they can start a new sheet. But to do so first they need to certify and close the current list of transactions with an unique key, that is approved by everyone in the group. Once they put a sheet in the envelope, it stays there forever, and cannot be changed anymore.

Basically that's it: a sheet of paper is a block of transactions, the envelope is the blockchain, and the process of closing and the certification is the bitcoin "mining".

Understanding the way how the certification and closing of the "sheet" is done is a bit more difficult. Let's imagine, that we have a encryption machine (hash algorithm), that nobody knows, how exactly works, but each time we put something in it, it returns the same encrypted value. For example, if we put the number 3 in it, it will always return "v0m7LKJf", but since nobody knows how it was generated, we cannot recover the input from the output. Now let's ask the following question: what should I use as an input, if I want to receive something on the output side, that starts with three zeros, like "000fke7DFc"? Decrypting "000fke7DFc" is not allowed, because the machine has no such feature, but we have an option: we can start putting random variables in the machine, till we get an output, that fulfils our requirements. It might take a few attempts, but once we have the input value, we can check anytime, if it still returns an output that starts with three zeros. This is exactly the logic behind certifying the sheets David, Adam and Tia have to put in their envelopes.

For example, if they would like to certify the sheet with number 15687 on it and they agree, that the secret code for the certification should be a number, that if they add to 15687, and then entering the result value into the encryption machine, it should return an output starting with three zeros (or anything else, that they agree on). As a start, they all start trying numbers randomly, till Adam finds 98762, which added to 15687 gives an input value of 114449, that returns "000vsdI3fF" by the machine. Adam shouts out loudly the number he found, so David and Tia can check its validity too. In case it really returns something starting with "000" for all of them, then it means, that the certification number is correct, so everybody

can put a stamp to sheet number 15687 with 98762 written on it and they can put it in their envelopes.

But what, if David says, that the certification code added to the number on the sheet does not return anything starting with three zeros for him? It can only happen for the following reasons: maybe he did not hear correctly one of the transactions initiated in group, or he incorrectly entered it on his sheet, or he tried to change one or more of the transactions in the list. In such cases, he is not allowed to put his sheet in his envelope, but he needs to throw it away. But then, he could not participate in the group neither, because all sheets must be in the correct order in his envelope, and he would miss the one, which was not certified. He can still ask Tia, if he could copy her sheet to be able to keep on working with them. But it would raise the questions, why should someone bother trying to find the correct encryption codes, if he or she can copy the result anytime from someone else in the group. The answer lies in incentives: to keep the participants motivated in the mining, the one who finds the code first, receives a reward in bitcoins. This is exactly why people mine cryptocurrencies, because they can earn additional ones by doing so.

One last thing, that needs to be mentioned: what if someone takes out an old sheet from the envelope, changes the transactions on it, and then searches a new certification code himself, that results in an encrypted output which starts with three zeros? The creator of the blockchain thought about this issue in advance, and instead of using an input value which is only a sum of two numbers (one that is given, and another that is mined), the sum of three numbers must be used for encryption: a number that reflects the number of transactions on the sheet, another number, which is the number of the previous sheet, and a third one which is mined. In this way the certification number of a sheet is connected to all the certification numbers of sheets coming after in the blockchain, which all should be adjusted, in case of changing a number in the middle of the chain.[35]

# Chapter 6. - Risks of the blockchain technology

Now that we know how the logic behind the blockchain was born, what historical milestones it went through and how the advantages of the technology evolved, this chapter will highlight the major risk factors of the system. Since it has some quite significant vulnerabilities, it is advisable for anyone planning to invest for example in bitcoin to familiarize beforehand with the risks brought by the crypto world.

## 6.1 - Is it a problem to be unregulated? Possibilities for manipulation?

One of the most serious weaknesses of the crypto network is, that there is no generally accepted **supervisory board** monitoring the trades and providing simultaneous protection to investors, which opens the backdoor for fraudsters. There are “traditional” ways for market manipulation, that are considered to be illegal by the S.E.C. and the F.S.A. in regulated frameworks like the NYSE or the London Stock Exchange, but can work well in the

[35] Farkas Dezső, 19 November 2017, “Hogyan született a Bitcoin, avagy a kriptovaluta és a blockchain rejtélyes világa”, http://jovotepitok.hu/hogyan-szuletett-bitcoin-avagy-kriptovaluta-es-blockchain-rejtelyes-vilaga/

blockchain network. The time frame of such scams can vary from really quick (it can take up to a few minutes in some cases) attacks to longer ones that might need days or weeks, but the damages caused to investors in both cases can be tremendous. The most often used technique is the "**Pump and dump**" strategy, which can be carried out in two ways:

- **Indirect Pump:** it is coordinated by a small group of insiders, who start buying a previously agreed cryptocurrency and by doing so they pump up the price. This so called first wave of trades generates signals to the market, that the security should be urgently bought, which is followed by a second wave of transactions by ordinary investors, who do not know anything about the manipulation they got into. Once the two waves have generated a high enough price, the investors of the first wave start massively selling their previously purchased cryptos to take the profit quickly. As a consequence of cashing out and putting back the cryptos to the market the price drops, making the second wave of investors losing money.[36]

- **Direct Pump:** the mechanism of the scam is more or less the same as for the indirect pump, but instead of a coordinated buying strategy, the manipulation starts with direct marketing approaches through social media and other communication platforms. Most of the time the messages scammers spread to credulous people are fake news and investment advises about instantly starting rapid price increases of specific cryptocurrencies: ergo you should invest now. Since it is also a kind of social engineering technique, online advertisements and chat groups are the most commonly used way of generating waves of direct pumps. Again once the fraudsters were able to pump up the price high enough, they start selling their previously purchased securities to cash out the profit and making ordinary investors losing money.[37]

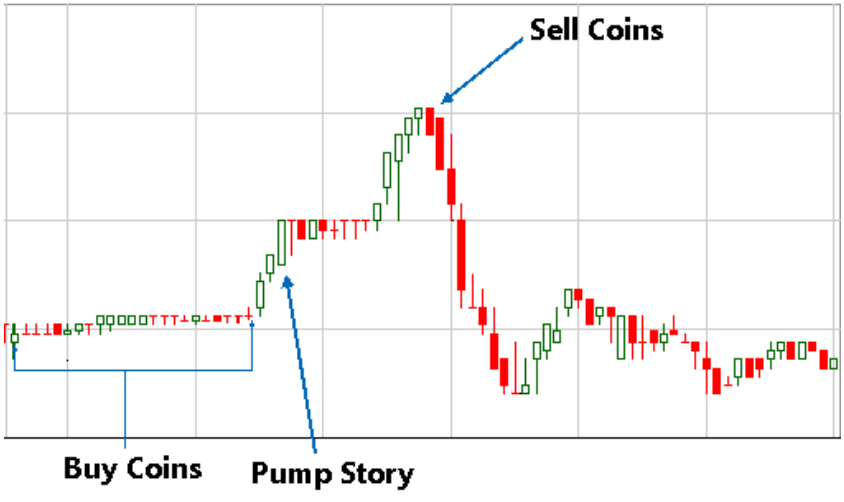



Image source[38]: https://restislaw.com/cftc-crypto-pump-dump-whistleblower/

[36] Adam Badenhorst, 10 December 2017, "Risks in an unregulated crypto market", https://currencies101.com/risks-unregulated-crypto-market/
[37] Patrick Thompson, 24 February 2018, "Pump and Dump in Crypto: Cases, Measures, Warnings", https://cointelegraph.com/news/pump-and-dump-in-crypto-cases-measures-warnings
[38] William Restis, 19 February 2018, "Whistleblower Awards From Cryptocurrency Pump and Dump Schemes", https://restislaw.com/cftc-crypto-pump-dump-whistleblower/

### 6.1.1 - The "50% +1" rule and the role of Mining Pools

The pump and dump manipulation technique is a weakness originated mainly from underregulation, but there are other vulnerability sources embedded in the system itself. First of all coins are granted as a reward only to the winning miners, who find the encryption key before anyone else. As a result and due to the size of the blockchain network, if someone would start mining on his own as of today, his or her chances to be the winner of the 12.5 BTC (which is the current block reward given away every 10 minutes) would be extremely low. In the end of the day it would just not worth investing time, effort and resources in cryptos, since it cannot generate a stable source of income. To increase the frequency of payouts, **mining pools** were invented as a solution. Mining pools are basically groups of people combining forces of thousands of computers, who are trying to solve these mathematical calculations together, and in case anyone of the pool finds the encryption key, all the other participants of the group gets a proportion of the awarded cryptos. As a result, individual miners receive a constant but lower income, which makes it more attractive for smaller bitcoin mining investors. The only problem with this approach is, that the three biggest mining pools cover more, than 50% of the overall mining capacities of the World, and according to the rules of the blockchain network only 50% consensus is needed to certify the blocks before they can be closed and stored. Of course it is only a theoretical threat, but with a bit of synchronization among the biggest mining pools, the whole blockchain could be altered. On top of this, more than **80% of all mining pools are located in China**, which makes the coordination even easier and therefore the risk higher.[39]

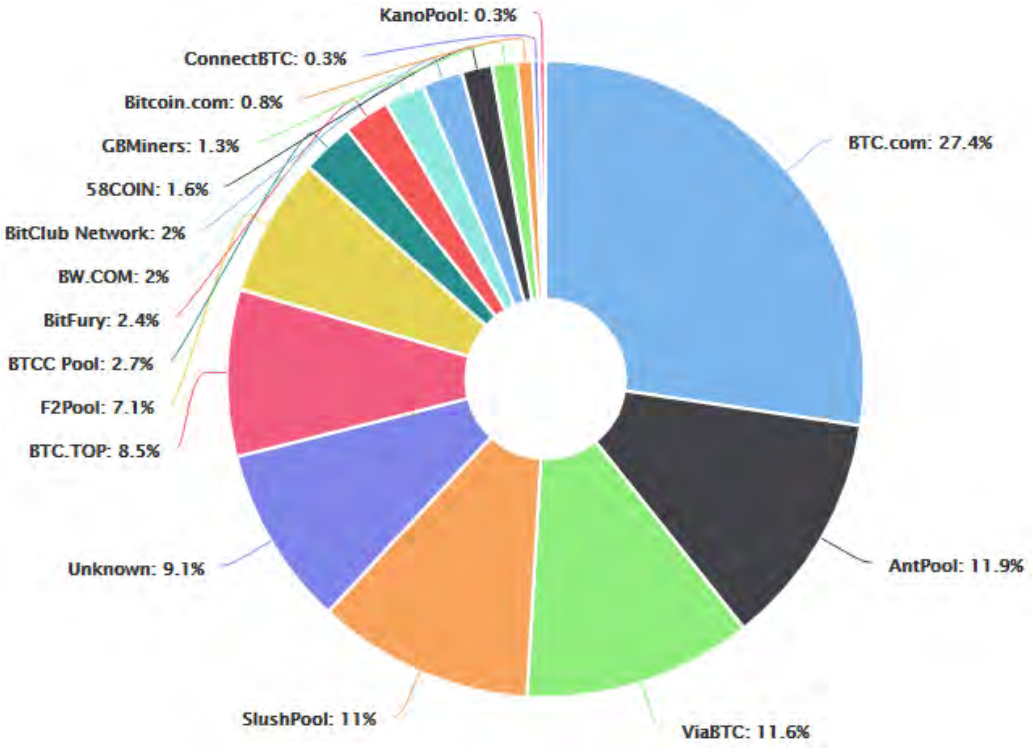



Image source[40]: https://blockchain.info/pools

[39] Kapersky Lab, 18 August 2017, "Six myths about the blockchain and Bitcoin: Debunking the effectiveness of the technology", https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/
[40] Blockchain Luxembourg S.A.R.L., 9 April 2018, "Hashrate Distribution", https://blockchain.info/pools

### 6.1.2 - ICOs and liquidity risk

Next to embedded vulnerabilities and market manipulation, there is a third type of risk in the blockchain network. Initial Coin Offering is a great tool to generate liquidity for projects and startups by exchanging ICO tokens for cryptocurrencies, but it also has some downsides, that derive mainly from underregulation. On one hand lots of scam or non-professional ICOs have appeared on the market with the bitcoin boom, however no selection were applied to separate them from the genuine ones. It is actually a notable issue, as it makes it more difficult for investors to be protected against poor projects and to find the ones, that have real value.

On the other hand lack of selection is not the only problem with ICOs, but another breed of risk has turned up lately, namely liquidity risk. Where the investment horizon of an ordinary IPO investor, who really believes in a project changes between 5 and 10 years, an average ICO speculator would keep his or her choice of asset in the portfolio for less, than 12 months. The problem with this investment behaviour is, that the vast majority of startups do not even have the chance to start operating or to become profitable with such a short notice, and as a consequence, if the "shareholders" want to cash out their invested amounts, they might face difficulties finding buyers for the tokens of an immature project.[41]

All together, the possibilities of market manipulation, mining pools, which we can also see as a form of cartels, combined with liquidity risk and lack of selection on the ICO market highlight the major risks what **underregulation** can bring.

## 6.2 - Environmental impacts and the power needs of Bitcoin Mining

The two fundamental requirements of having the blockchain technology available today are internet and computers. While its bandwidth needs are not significant, its computation requirements are constantly increasing along the growing network of crypto users. According to a report of the International Energy Agency in the end of 2017 bitcoin mining has been using as much electricity as smaller countries like **Serbia**, and blockchain specialists forecast the power consumption level of the US to be needed for maintaining the system by 2019. Therefore electricity prices have a direct relationship with bitcoin mining, because people will only stay motivated in allocating their computation resources for processing, if the income they can generate is higher, than the electricity costs they need to pay.[42]

[41] Jamie Burke, April 2017, "ICO Pros & Cons: Cutting Through The Hype", https://outlierventures.io/research/cutting-through-the-ico-hype/
[42] Adam Rogers, 15 December 2017, "The hard math behind Bitcoin's global warming problem", https://www.wired.com/story/bitcoin-global-warming/

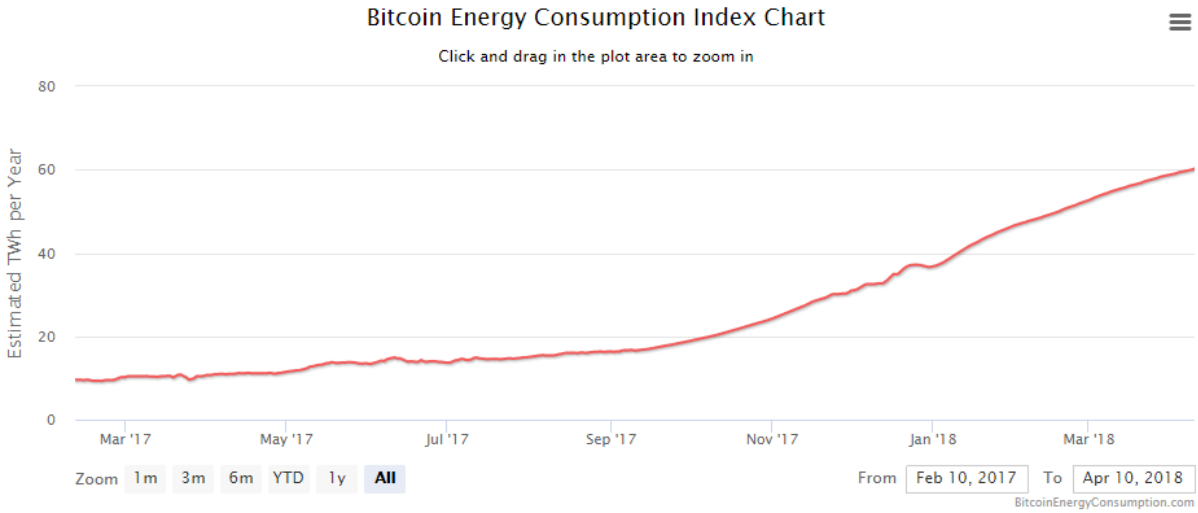



Image source[43]: https://digiconomist.net/bitcoin-energy-consumption

It also implies some indirect sources of risk for bitcoin holders: in case power consumption fees show a more steeply increasing trend compared to revenue generated by bitcoin mining, less and less people will allocate their computation resources for maintaining the blockchain network (since the margin is getting smaller), and after a while crypto transaction processing will slow down. As a consequence bitcoin usage will also decrease as it will be less advantageous, than traditional means of payment, which delineates lower demand for cryptocurrencies, what will result in a decline in their prices. Lastly bitcoin and any other alternative coin holders will be facing a loss on their investments.

All in all there is a strong correlation between energy prices and the blockchain, that just confirms importance of alternative energy resources.

### 6.2.1 - Is it a sustainable way of doing business?

At the moment it is difficult to tell: various online literatures have already tried to forecast the future of bitcoin from energy consumption point of view, and the possible estimations often became the complete opposite of each other. Indeed there are innovations, that are triggered by the technology, like faster CPUs, stronger graphic cards and also dedicated mining machines, that can initiate more computations next to higher effectiveness. But does this also mean, that we will put an end to our hardware needs because we can cover the same requirements with less hardware? Probably not, because people with resources will always try to exploit the most for their benefit.

But what, if bitcoin usage will just keep on increasing exponentially in the coming years? Or what, if the blockchain technology will go through a innovative revolution, that we cannot foresee at the moment, but will change its power requirements completely? Or if there is a shift in power prices? These are the major factors, which need to be taken into consideration, if we would like to forecast the longer-term possibilities of sustainability of the blockchain network.

[43] Digiconomist, 11 April 2018, “Bitcoin Energy Consumption Index”, https://digiconomist.net/bitcoin-energy-consumption

Thus innovation combined with sustainable energy resources will play a significant role in the future of cryptocurrencies. Fortunately there are already very original approaches in bitcoin mining: entrepreneur Marco Streng for example has setup one of the biggest and most environmentally friendly mining farm in Iceland, with more ten thousands of graphic cards running 24/7. His choice of Iceland as the home of the startup was on one side due to the country's geothermal power plants, which produces cheap and green energy from hot springs. On the other side the weather characteristics of the country helps cooling the computers in a natural and eco-friendly way.[44]

With innovative and progressive solutions the network might be sustainable, but they also draw up possible sources of risk, that might have such impact which is currently undetectable: for example the risk of innovation. Computation speed has always been a key factor in cryptocurrency mining, because the quicker we find the encryption key of a block, the more we can earn, but too much speed could be dangerous for the system too. As of today quantum computers do not exist yet, but with the rapidity of innovation we face in the digitalization era, they might become available in the near future. That would mean the end of the blockchain, because a computer, that can re-encode blocks faster, than the network encodes them, would open the backdoor for transaction manipulation.

I believe, that the system can be maintained on the long run, if the demand for cryptocurrencies will meet the necessary conditions, but it also depends on endless number of variables with different characteristics for each and various correlation among them.

### 6.3 - Explaining the sources of volatility of the bitcoin

In the end of 2017 bitcoin was traded around $20000 and three-four months later it is varying between $6000 and $10000, so it cannot be called as a stable security at all. Of course these price fluctuations are always the product of several factors, and it would be an endless list, if we would start mentioning them, but as always there are some major drivers we can name, that has the biggest impact on volatility:

**Speculation**: in the end of the day blockchain is just a peculiar way of transferring money from one person to another and nothing else. It does not pay dividends or interests as regular stocks and bonds, and it has no intrinsic value neither. It is not like ordinary shares of corporates with real production behind, what could motivate people to hold a security for a longer period, but in fact it is only the belief in the technology, what assigns value to bitcoin and altcoins. As a consequence price movements are primarily driven by people's speculation (by their demand and supply), according to their assumption if they think it will go up or down. Therefore a bigger proportion of the volatility of cryptocurrencies are artificially generated by price conjectures.[45]

[44] Julian Mitchell, 15 December 2016, "Meet The 27-Year-Old Mathematician Building A Bitcoin Empire", https://www.forbes.com/sites/julianmitchell/2016/12/15/meet-the-27-year-old-mathemetician-building-a-bitcoin-empire/#2b960afd1d74
[45] Jay Adkisson, 9 February 2018, "Why Bitcoin Is So Volatile", https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/2/#164c9b6790de

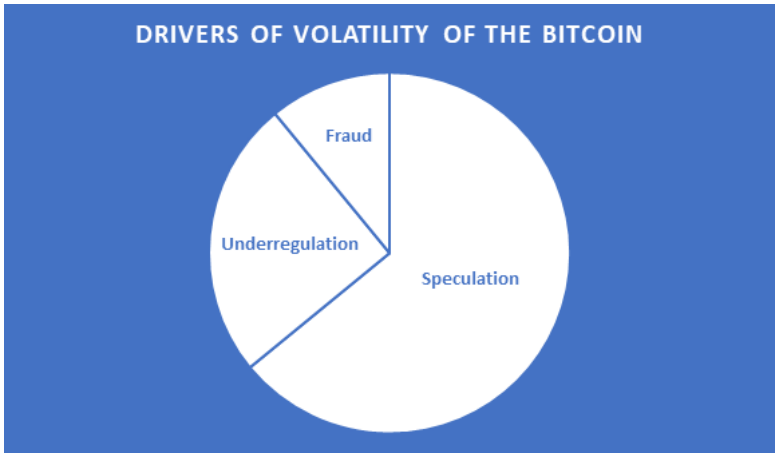
**Lack of regulation**: As explained before, there are many ways for price manipulation in the blockchain network (like the pump and dump strategy), which would not be possible in regulated frameworks, because those would provide protection to investors. The goal of these activities is to artificially change the price, ergo to increase volatility and to cash out the profit on the expense of other cryptocurrency holders. Even if we are facing a constant decline in bitcoin prices for the last three-four months it occasionally happens, that group investors start false signaling the market in the opposite direction (so called bull trapping strategy), making people believe, that we have reached the bottom of the shortfall:


Image source[46]: https://transportgeography.org/?page_id=9035

**Fraud**: With the increasing popularity of bitcoin it became the centre of attention of fraudsters too. In reality blockchain is a secure system, but the services built around it are far from that. All in all the network is still too young and not part of the traditional bank system, that has well established security measures and strict protocols to follow and for this reason crypto wallet providers and crypto exchanges are full of security gaps. Undoubtedly it generates nonstop threat for crypto users, since hackers are constantly seeking for vulnerabilities, and they are obviously not afraid to exploit them. Just to mention an example, the security breach of the crypto exchange Mt.Gox resulted in a loss of $400M for their clients. When such fraudulent cases turn up in the media, serious number of bitcoin holders cash out their investments immediately to avoid potential losses, which have direct impact on the market, making cryptos more volatile.[47]

[46] Jean-Paul Rodrigue, 2017, "The geography of transport systems", https://transportgeography.org/?page_id=9035
[47] David Drake, 2 March 2018, "What is making bitcoin so volatile?", https://irishtechnews.ie/what-is-making-bitcoin-so-volatile-insights-with-david-drake/

In short the biggest proportion of bitcoin volatility derives purely from speculation, but lack of regulation has also a significant impact on rapid price movements. Fraudulent activities shifts the demand curve of the blockchain also in a negative direction, but it is only an occasional factor compared to the previous two ones, as it requires media attention to be convincing enough to start a wave of massive selling.




### 6.3.1 - Do big hedge funds invest in bitcoin?

For the time being institutional investors preferred to be careful and stayed away from the bitcoin market, but a sharper shift is expected to take place during 2018 because all the signs clearly point to the direction of hedge funds having cryptocurrencies included soon in their portfolio: as a first step in the end of 2017 Chicago Mercantile Exchange (CME) introduced futures contracts on bitcoins, then the interest encompassing them also showed a significant increase of 64% in the last four months (from ~1600 contracts bought per day to ~2500 contracts as of today). Due to the high level of demand thanks to the media followed by pressure on market regulators, it is only a matter of time till bitcoin will also be publicly traded. As a consequence cryptocurrencies will have access to a **huge ocean of wealth**.[48]

However the crypto market in first place is still dominated by individual investors, what generates extreme volatility in bitcoin prices. On average the investment horizon of an individual investor is much shorter, than institutional investors, because they are not following, the buy-and-hold strategy, which would be essential to provide stability for security prices, but they are more like speculators and day-traders. In regulated financial markets long-term investors, who hold an asset for years play a significant role to provide stability for the underlying and to reduce general volatility of the assets.[49]

The following chart shows, that the stability of cryptocurrencies is far from the traditional securities, what can be found in the portfolio of institutional investors. For example the difference between the 60-day BTC/USD volatility compared to the 60-day USD/EUR volatility is around 5:1 - 8:1 in general. Where the daily standard deviation from the mean for

[48] Laura He, 11 April 2018, “Demand from institutional investors drives up bitcoin futures trading volumes on CME”,
http://www.scmp.com/business/markets/article/2141119/demand-institutional-investors-drives-bitcoin-futures-trading
[49] Jay Adkisson, 9 February 2018, “Why Bitcoin Is So Volatile”,
https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/2/#164c9b6790de

major currencies fluctuates between 0.5% and 1.00%, it is around 4.70% on average for bitcoin. In extreme situations, for example when bitcoin was traded close to $20000 in the end of 2017, the volatility of bitcoin was almost 8.00% while it was 0.40% for USD/EUR (20:1).

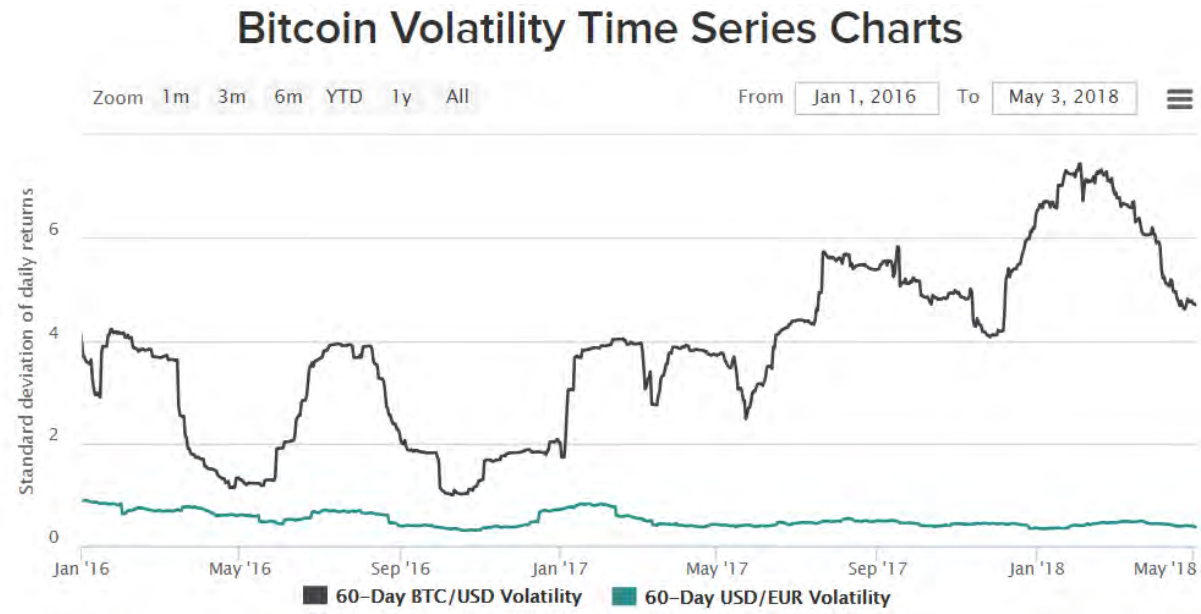



Image source[50]: https://www.buybitcoinworldwide.com/volatility-index/

## 6.4 - Security risks of the blockchain technology (including historical examples)

As it can be seen on the volatility chart the dominance of individual investors is a risk by itself, but it also puts a huge pressure and administrative workload on crypto wallet providers and crypto exchanges. To mention a few examples Binance.com has 250.000 new account registrations on a daily basis, while Kraken.com also receives 50.000 per day and Bitfinex.com together with CEX.io had to stop onboarding new clients to be able to catch up with the dumping of users. With the speed of non-institutional investors rushing to the market, there is also higher risk of security breaches, as the service providers cannot keep up with fixing all the vulnerability points of their systems. All in all the hype around cryptocurrencies also contributes with a boost to the already not moderate volatility of bitcoin.[51]

Mainly due to increased number of security breaches, where bitcoins were stolen by hackers the vulnerability of the blockchain is a popular topic for defamation. In this chapter I intend to highlight the fact, that this type of thinking is equivalent to saying that Dollar is not secure enough, as many Dollars were stolen in the past. It is important to mention that the blockchain itself has proved many times, that it is a safe network and the security risk of the system originates mainly from the human factor: on one side it depends on how

[50] Buy Bitcoin Online, 3 May 2018, “The Bitcoin Volatility Index”, https://www.buybitcoinworldwide.com/volatility-index/
[51] Alexander Kravets, 18 January 2018, “Institutional Investors Will Bet Big on Cryptocurrencies in 2018”, https://cointelegraph.com/news/institutional-investors-will-bet-big-on-cryptocurrencies-in-2018

confidentially crypto holders handle their cryptos, and on the other side on how up-to-date service providers are with the latest security measures built around the technology.

### 6.4.1 - Does it really provide anonymity for the user?

Rule number one for cryptocurrency holders: never share the private key of your crypto wallet with anyone. Having the private key of a wallet means full control over the cryptos on it. Obviously it is not so easy to avoid giving it out to third parties as in most cases individual investors must rely on crypto wallet providers to be able to buy or sell bitcoins and altcoins. But in this case already two parties (the wallet provider and the account holder) have access to the private key, which also means, if the provider would like to steal cryptos from their clients, they have all the possibilities to do so. It is similar to putting an amount in the bank, where the money itself is not in the account holder's property anymore, therefore he or she lose direct control over it. Fortunately banks are highly regulated firms, where crypto wallet providers are not yet.

The other problem with the involvement of third parties is in relation to the "myth" of bitcoin being an anonymous form of payment, because in reality blockchain is a pseudonymous network. After the general ledger is publicly accessible for anyone and all the transactions are stored in it, bitcoin addresses can be easily traced back. The risk of this is, if the identity of someone can be linked to bitcoin addresses, then all the incoming and outgoing transfers can be looked back for that given person. Consequently it is important to choose reliable crypto wallet providers, because they do initial KYC checks during the account opening process and they keep information about the identities of all their clients. If it is really important for us to hide our identity and to make it difficult to trace back the origin of our funds, mixing services and different wallet providers can do the job for us. Mixing services are basically aggregated wallets, where crypto holders need to send the funds to one big account of the provider, so it can "mix" the incoming transfers of different clients. Then the provider periodically initiates payments to the recipients selected in advance, therefore it will be difficult to link the senders to the receivers. These solutions still not provide complete anonymity, but with a bit of security awareness our identities can be kept protected.[52]

### 6.4.2 - Lost bitcoins

As of today we have two ways of losing bitcoins or any other cryptocurrencies. Either we forget the private key of the wallet where we store them, or we became victims of theft by hackers. The first case might not sound a serious issue, but we definitely need to take it into consideration when we talk about the risks of the blockchain technology, because in reality a significant proportion of the global bitcoin stocks belong to this category. Already in 2015 30% of the overall bitcoins ever mined were considered as "dormant", which means they were not used at least for the last one and a half year. This does not mean, that they are lost, but there is a high chance, that many of them will not be recovered ever. One of the most famous cases of lost bitcoins happened to James Howells, a Welsh developer, who has thrown away his hard disk including the private key of his wallet, which had 7500BTC on it.

[52] Jordan Tuwiner, 2018, "Bitcoin Anonymity - Is Bitcoin Anonymous?", https://www.buybitcoinworldwide.com/anonymity/

Unfortunately he had no way of getting back his acces, what on today's price means a loss of $60 Million.[53]

Of course even crypto wallet providers have two types: ones that store private keys on behalf of their clients and ones that do not. Both of them have their advantages and disadvantages. For example with providers, where the private key is stored, people do not need to bother with remembering it, but there is a risk if the servers of the company is breached, hackers will have full control over the money. In contrast this risk can be eliminated by providers, which let their clients protect their private keys, but then it is the user's responsibility not to lose it.[54]

Regarding losing cryptocurrencies through criminal cases: since bitcoin due to its exponentially increasing popularity became the centre of attention for fraudsters, it has opened blue ocean markets also for cyber security startups. Most probably the solutions of these newly established companies will mature over time, but as of today there are some leakages in the services they built around the blockchain network: in November 2017 a vulnerability was found in the code of ethereum by IT-Sec company, Cisco Talos, that resulted in a leakage of $155 Million. A month later in December a South Korean crypto exchange, Youbit went bankrupt after hackers have stolen 17% of the assets of their clients in value of $63 Million. These are just two examples how vulnerable the peripheral services of the blockchain network is, and without the necessary security improvements hackers will remain active in the industry.[55]

### 6.4.3 - AML and Terrorism funding involving the technology

The bad reputation of the blockchain originates from bitcoin being the preferred payment method on the dark web for purchasing drugs and weapons. Undoubtedly the network (mainly in its earlier years) was started to be associated with money laundry and terrorism funding as a consequence, but in reality it is not as obvious how it can support these illegal activities. Indeed, the platform can help both "businesses" as the underlying technology have particularly favorable features for them, but there are some pivotal points in the system, that makes its usage risky for fraudsters and terrorist.

Let's start with the pseudonymity aspect. As explained before it is a common belief, that large amounts can be transferred quickly from one place to another without revealing the identity of the sender and the receiver. True, but as long as the general ledger is publicly accessible for anyone, noone is really anonym in the network. Converting cryptos to local currencies is also an extra barrier in terrorism funding: for example Syria and Iraq not being supported by the major crypto exchanges forces people to have American, European or Chinese exchanges involved in the fund withdrawal process. These exchanges already

[53] Matthew Sparkes, 23 January 2015, "The £625m lost forever - the phenomenon of disappearing Bitcoins", https://www.telegraph.co.uk/technology/news/11362827/The-625m-lost-forever-the-phenomenon-of-disappearing-Bitcoins.html
[54] Sudhir Khatwani, 29 March 2018, "Bitcoin Private Keys: Everything You Need To Know", https://coinsutra.com/bitcoin-private-key/
[55] Olga Kharif, 18 January 2018, "Hackers Have Walked Off With About 14% of Big Digital Currencies", https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies

require an initial KYC for opening an account with them, hence anonymity is lost for their clients. Finally, when the funds are converted to local currencies (apart of the forbidden ones) and they reach the traditional banksystem, they can be easily tracked.[56]

All the above shows the importance and the need of regulation in the blockchain world: French Finance Minister Bruno Le Maire together with Italian Finance Minister Pier Carlo Padoan have already called for discussions around the topic of virtual currencies and urge for global regulation. Their views were also shared with European Commission vice president Valdis Dombrovskis, and Stephen Barclay, Economic Secretary to the British Treasury and as a result a meeting was called together in Brussels on 20. February 2018. The outcome of the discussions was mainly a proposal to make the AML directives applicable for crypto exchanges and wallet providers, which will also be used during G20 meetings later this year in Argentina.[57]

# Chapter 7. - Introduction of the PSD2 regulation

The topic of the following four chapters will be a little bit different from the previous ones, as its main objective is not to explain anything about the bitcoin or the blockchain technology, but to illustrate some changes coming soon into the traditional banksystem of Europe, that might have some serious impacts on the future of cryptocurrencies as well. These improvements envisage financial technologies within the European Union to be kept up to date with the latest market trends.

## 7.1 - History of the Payment Service Directive

PSD1 or the Payment Service Directive was published by the European Parliament and European Council on 25. December 2007 and set its due date to be implemented by the member countries into their own legislation by 1. November 2009. It remained effective for a bit longer, than ten years till 13. January 2018, when it was replaced by an upgraded version of it, the PSD2. PSD1 was basically guideline or more accurately a set of rules, that set the creation of a single market of payments in Europe and the establishment of the Single Euro Payments Area (SEPA) as its primary goal. It also meant to lift the speed, easiness, security and costs of cross-border bank transfers, direct debit and card payment operations to the level of domestic payment solutions. The directive influenced the European market into the direction of better customer protection and services through its three main pillars as follows:

- **Pillar I - Licensing requirement:** According to PSD1 all payment service providers (PSPs) within the European Union had to hold a PSD license to be able to operate payment related activities. To do so each member state had to delegate specific tasks to their competent domestic financial organizations, which were responsible for issuing the licenses in the new framework. As a result of the directive, the appointed

[56] Kai Sedgwick, 10 December 2017, “Despite What Politicians Say — Terrorists Don’t Use Bitcoin”, https://news.bitcoin.com/despite-politicians-say-terrorists-dont-use-bitcoin/
[57] C. Edward Kelso, 2 March 2018, “EU Losing Patience – Urges Global Crypto Regulation”, https://news.bitcoin.com/eu-losing-patience-bitcoin-needs-global-regulation/

legal bodies could only have approved the PSD license request in case, if the applicant financial institution implemented well established corporate governance protocols into their businesses and had sufficient capital available for supporting their operations.

- **Pillar II - Notification requirements:** According to the new legislation, payment service providers in scope must have provided clearly understandable information to their clients before and after they provide payment services to them:

    - Before the payment took place, PSPs must have informed their recipients about all the costs of their services, the procedure of handling disputes and also about the final amount to be paid by the customers.

    - After the payment took place, payment providers must have informed their clients about the reference identifier of the payment transaction (Transaction ID), that also contained necessary information to confirm the payer, the cost of operations and the final amount paid.

    - PSD1 has also provided guidelines for further obligatory requirements regulating recurring payments agreement between the payment service provider and the customer, that authorized future payment operations (debits) with the consent of the client initiated by the PSP.

- **Pillar III - Rights and obligations:** To boost the speed of cross-border transactions and to take a leap into the direction of a single European payment market, PSD1 enforced to have all payments in Euro or any other currencies of the member countries outside the eurozone to be processed within one day:

    - As a strict obligation originating from the directive, it held payment service providers fully responsible for providing flawless transaction processing services. In case of occasional payment processing errors or service not provided, PSPs had to fix the issues as soon as possible or to compensate the customer up to the amount previously paid. If payment transactions were initiated and authorized by the given financial institutions by mistake, they must have provided proper solution for issuing refunds to the payer in question.

The directive was in place for more, than 10 years, but getting closer to the end of its lifetime, it crystallized, that a bit more detailed guidelines were necessary, as the digitalization era brought sophisticated new innovations into the payment world, while many of them have already laid outside the scope of PSD1. Therefore in the beginning of 2018 the advanced version of the directive, PSD2 was introduced.[58]

[58] European Parliament and European Council, 13 November 2007, “Pénzforgalmi szolgáltatások az EU-ban”, http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33226&from=EN&isLegissum=true

### 7.2 - Innovation brought with the PSD2: the appearance of PISPs and AISPs

The main goal of the PSD2, including all the advantages derived from previous objectives of the first directive was to provide a regulated framework for these innovative newcomers on the payments market. The logic behind was to further strengthen competition within the EU so customers could have chosen from a bigger variety and cheaper services next to maintaining industry standards. As a first step, the schema provided guidelines for the member countries forcing them to register, license and regulate these new payment institutions. As a second step it has also extended the geographical coverage of the operations in scope: while PSD1 focused mainly on cross-border transactions in the currencies of member countries of the European Union, PSD2 has added all currencies to its portfolio. To make it fully compliant with the latest market needs, it covered also the so called "One Leg Out" transactions, where one payment service provider was located inside the European Economic Area, but the other PSP was outside of it. All in all the EU envisaged the obligatory implementation of the new measures into domestic law by 13. January 2018.

To be able to highlight the biggest differences between PSD1 and PSD2, it is important to mention, that several new types of third party providers appeared on the market altering the previously known payment flow. They were created as a result of the revolution of global eCommerce businesses, international mobile banking applications and cell phone optimized payment methods, like contactless (NFC) solutions. While in the traditional payment world the main parties of the payment process were the following ones:

- Banks: from one side the acquiring banks, that opened merchant accounts for merchants to collect the incoming payments and to initiate settlements, and on the other side the issuer banks, which provided the bank accounts and credit or debit cards of the buyers.

- Payment Service Providers: which were basically technical platforms or gateways connecting the buyers to the sellers.

- Card schemes: like VISA and MasterCard in case of card payments, which provided clearing for transactions.

PSD2 in contrast introduced two new types of service providers in the flow: the Payment Information Service Providers (PISP) and the Account Information Service Providers (AISP).

**PISP:** Payment Information Service Providers are special PSPs, who can initiate payments on behalf of their customers without having actually an account opened for them. They are technically an extra layer of service providers built on the basic services of issuer banks (or ASPSPs as they are called in PSD2: Account Servicing Payment Service Providers). To have these PISPs being able to do their activities, the account/card holders will need to provide permission to the PISP in advance to receive their bank account details, so then the PISP can connect to the system of the ASPSP through an API call (API: application program interface - the technical connection between the system of the issuer bank and the PISP).

The advantages of this kind of setup is, that there is no need for using credit or debit cards anymore to initiate a credit transfer, but it will be possible to do it directly from bank accounts.

As increased security risk is also involved in this new way of triggering payments, there are strict measures applied on PISPs to receive permission before they can start operating: they must hold a PSD licence of their domestic country, and they must also get passporting rights to be active within the EU. Once they received green light from the authorities to start processing, they must respect a long list of security requirements and privacy policies (which are regulated under the GDPR directives, being applicable from 25. May 2018), how to handle customer information and transaction data.

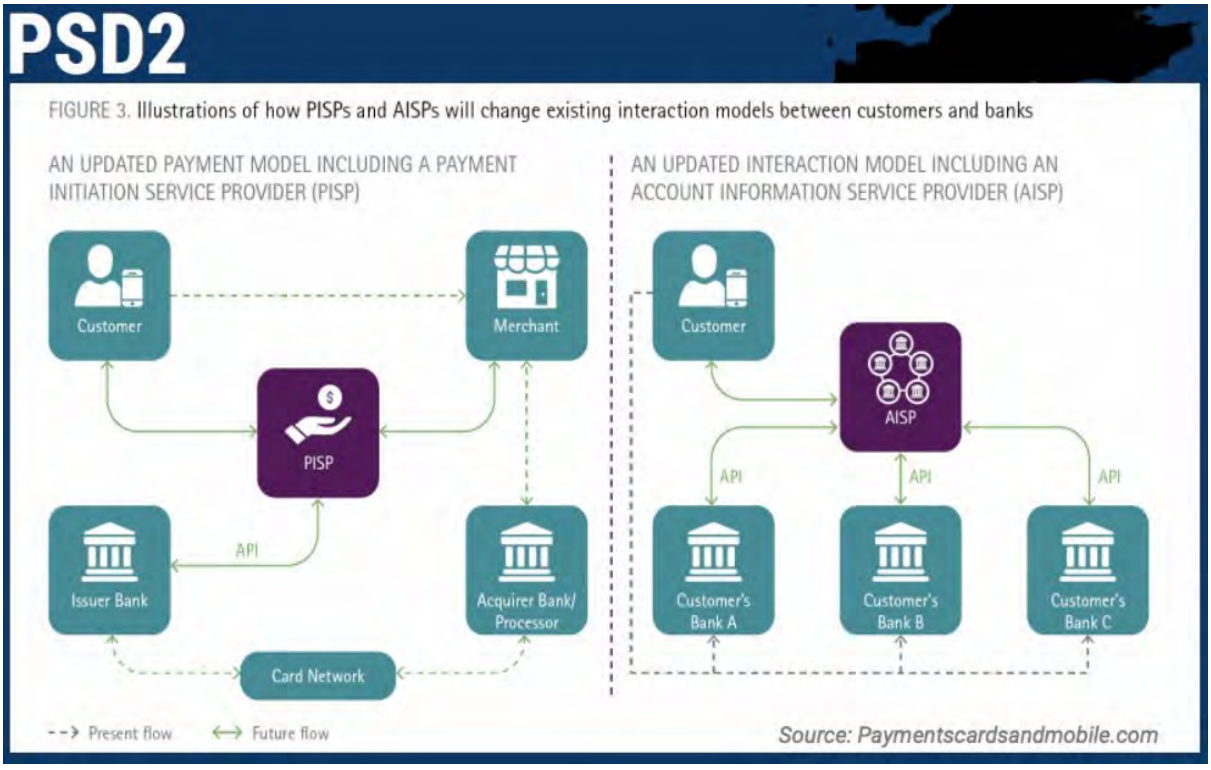



Image source[59]:
http://www.paymentscardsandmobile.com/wp-content/uploads/2016/05/Final-Accenture-Payment-Services-PSD2-PoV-Web-April-2016.pdf

**AISP:** Account Service Information Provider is the universal name for companies specialized in transaction information, account balance and account information data processing and handling. In contrast to PISPs, they cannot initiate credit transfers for their clients, but they are capable of providing them bank account information in an aggregated view. To explain better what they do, I made up a basic example: let's imagine, that a company has bank accounts both at BNP Paribas and Banque de Luxembourg and each time they need a consolidated report of incoming or outgoing funds, they need to login (most of the time with the help of a token due to security reasons) into the netbanking platforms of both banks, export the lists of transactions separately, then combine them in Excel or with any spreadsheet manager software. This is apparently very time consuming and also requires

[59] Payments, Cards and Mobile, 18 May 2016, ,"Opportunities unlocked by revised PSD2", http://www.paymentscardsandmobile.com/wp-content/uploads/2016/05/Final-Accenture-Payment-Services-PSD2-PoV-Web-April-2016.pdf

many passwords and tokens to manage. AISPs to help better managing bank account information will be able to handle everything in one aggregated interface, after obtaining explicit consent of their customers to get access to their bank accounts. These providers, since they are specialized in account information handling, will also provide several additional features like aggregated charts, reports, collective balances, and so on.[60]

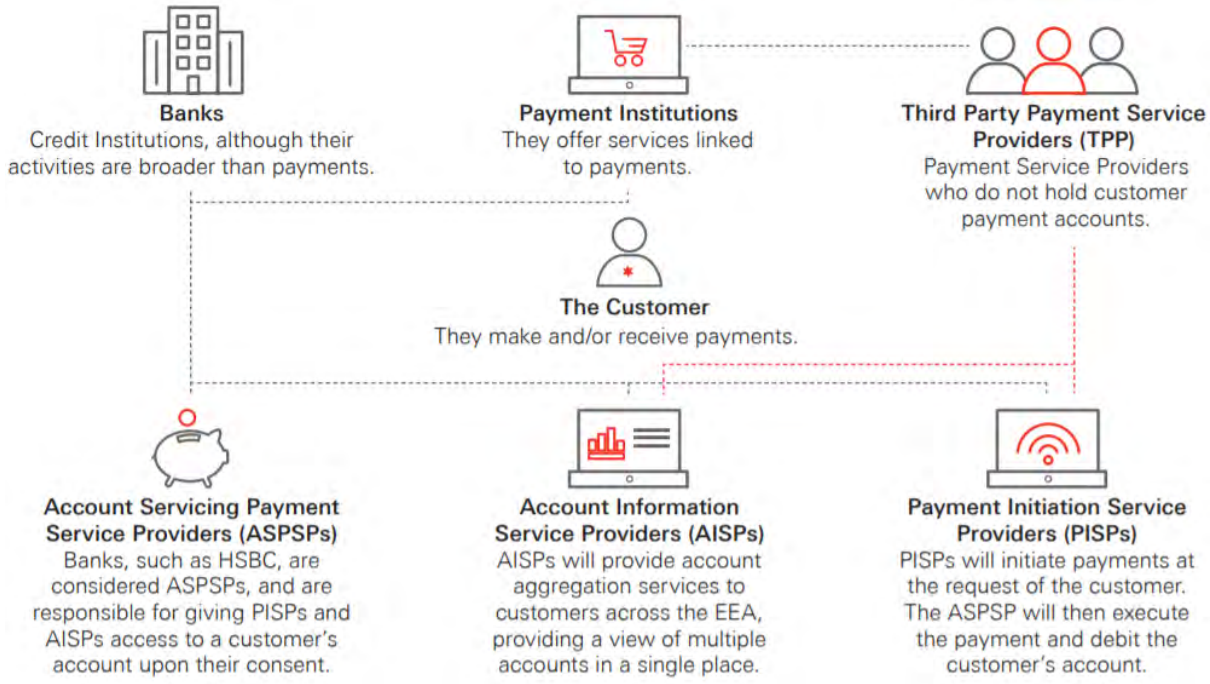



Image source[61]: http://www.gbm.hsbc.com/insights/technology/payment-services-directive-ii-psd2

**API:** API (or application program interface) is the generally accepted acronym for technical connectivity details of servers of banks or any other companies. According to the PSD2 framework, banks must open up their systems and make them accessible for PISPs and AISPs through their API in a way, that they should be capable of reaching such information and functionalities, what bank account holders have through their netbanking applications. While the deadline for publishing the technical documentations is 14. March 2019, the changes have already opened new possibilities for IT companies developing standardized APIs. As a direct consequence of more parties having access to confidential information, a new verification technique, the so called strong cardholder authorization (SCA) will have to be triggered each time a PISP or AISP request access to sensitive data. PSD2 also enforces ASPSPs to provide backup solutions for their API users, if the servers of the bank does not respond after five consecutive calls within 30 seconds: in such cases they must grant access to their netbanking platforms to help their users collecting the necessary data with screen scraping technologies. To avoid banks pulling back competition by making their API not accessible for PISPs and AISPs, they will also have to provide quarterly statistics about the availability of their netbanking platform versus their application program interface.[62]

[60] HSBC, 2018, "Payment Services Directive II (PSD2)", http://www.gbm.hsbc.com/-/media/gbm/reports/insights/payment-services-directive-ii-psd2.pdf
[61] HSBC, 2018, "Payment Services Directive II (PSD2)",http://www.gbm.hsbc.com/insights/technology/payment-services-directive-ii-psd2
[62] Nemeth Monika, 19. March 2018, "2019 márciusától elérhető lesz az összes banki API az EU-ban", https://fintechzone.hu/psd2-banki-api-2019/

The reason why I introduced the topic of PSD2 is, that I believe it will create a legal platform for innovative payment companies appearing on the market, that might provide alternatives to the peculiarities of the blockchain technology, but within a regulated framework at the same time.

### 7.3 - Closed loop platforms created by PISPs and AISPs

Discussing the PISP topic with Charles Fogg, founder of Bige Ltd. my conjecture seems to be proven, as he has already developed a system, that has similar characteristics to the blockchain by exploiting the advantages brought with PSD2. Exchanging several emails about his payment platform he described a closed loop network, Bige (www.bigeltd.com), which is a combination of PISP and AISP and by connecting to the APIs of banks it will support the following services:

*"We offer a closed loop transaction which indicates, that there are interactions between 2 or more internal elements without interference from the outside. In the financial sector it's often related to money transfers between accounts in the same financial institute. In the BigeFinancials case, then when issuing virtual accounts to both the merchant and the end-user, it is considered closed loop processing, as the transactions stays in the same closed network. When the end-user uses the eWallet account the transaction will be routed directly to the BigeFinancials platform and the transaction will be cleared and settled directly and instantly. The traditional payment network and card-schemes are not involved and the settlements can be performed instantly. Closed loop payments can be available for all Internet and mobile payments as well as NFC payments." - Charles Fogg*

The platform is basically a closed network like the blockchain, that provides instant payments (also like the blockchain) and any changes in payment amount make the authorization code invalid (similarly to falsifying the certification codes of the block). Finally it almost eliminates the costs normally associated with processing payments (again also like the blockchain).

To enter the network first card holders and bank account holders (can be a customer or a merchant) need to authorize Bige Ltd. to receive card or bank account details, and by doing so, the system creates Bige eWallets automatically for their users. Once it is done, the cashflow remains within the closed network of Bige (meaning among the e-wallets created) as long as there is no funding initiated or withdrawal requested. With this "trick" all transactions will act like interbank transfers, therefore all the recipients will get their payments instantly. When a Bige Wallet holder decides to fund or withdraw money from/to the closed network, Bige being a licensed PISP can initiate payments on behalf of its users from and to their private bank accounts without any interaction needed between the user and his or her bank. The value added features of AISPs come to picture, when Bige users have multiple cards or bank accounts: Bige Ltd. is also a registered AISP, meaning they can connect to more banks to extract account information for their clients:

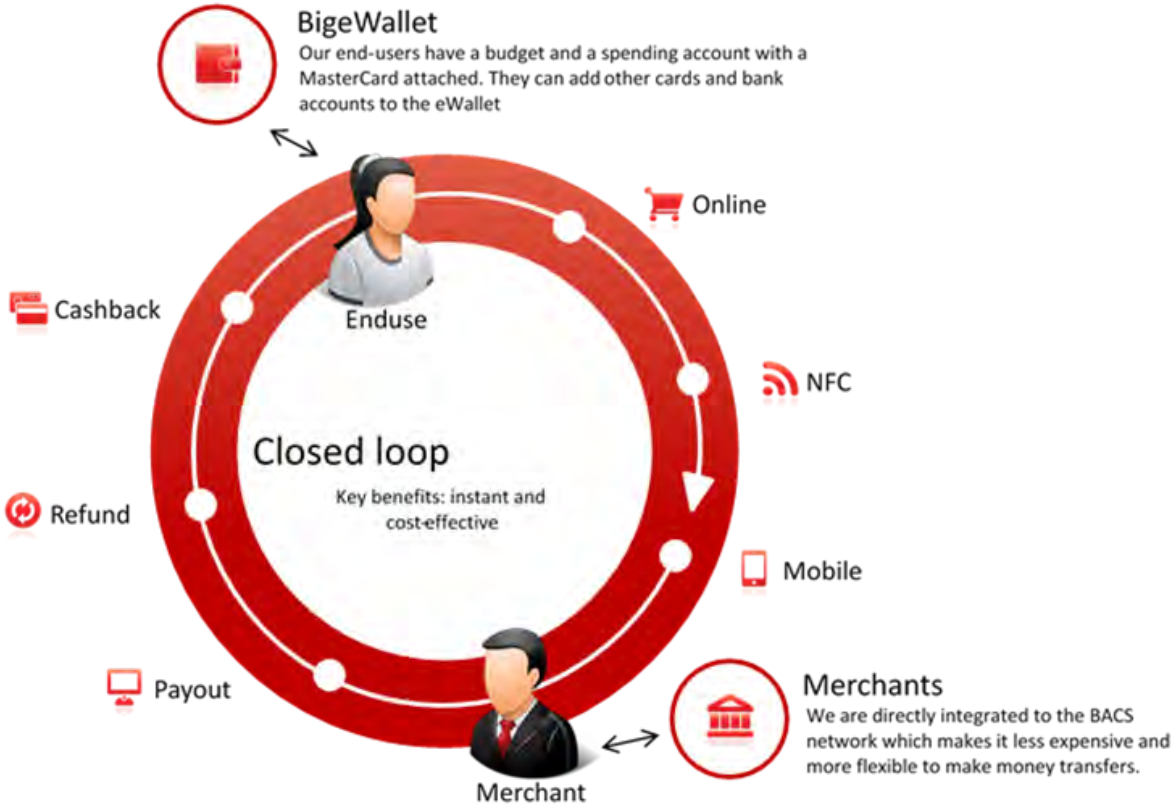



Image Source[63]: http://www.bigeltd.com/wp-content/uploads/2018/04/closed-loop-processing.png

The system technically combines the advantages of the blockchain and credit card payments in one standalone network:

- There is no need of entering credit card details at all

- Conversion rate is essential in credit card payments, which depends on several factors like:

    - The card issuer bank
    - The acquiring bank, where the merchant account is held
    - The geographical location of both banks
    - The MCC (merchant category code) of the merchant
    - Fraud measures, spending limits, blacklisted countries, etc.
    - SLA (services level agreement) of the payment providers, acquiring banks (having a 99.99% SLA versus 99.999% makes a big difference)

    where Bige Ltd. provides almost 100% conversion rate

- There is no need of reserves being held back by acquiring banks, where in card payments the industry standard is 5%-10% rolling reserve, or fixed collaterals

[63] Bige Ltd, 8 May 2018, “Bige Closed loop processing” http://www.bigeltd.com/wp-content/uploads/2018/04/closed-loop-processing.png

- Bige virtually eliminates the possibility of fraud due to transparency and implementing two factor authentication text verification on all transactions.

- Strong customer authentication through a closed loop environment which includes elements that 'dynamically link' the transaction to a specific amount and a specific payee.

Obviously these sound very well, but PSD2's main objective was to increase competition on the market for the benefit of end users, therefore such innovation most probably will have impact on the business strategy of crypto wallet providers, processors and exchanges too.

### 7.4 - Interactions between the blockchain technology and the innovative technologies created by the PSD2

To have a feeling about how crypto payment providers will react on industry changes and adjust their strategy for the future, I interviewed Lithuania based Coingate (https://coingate.com/), who offers bitcoin and tons of other alternative cryptocurrency processing:

*"Our company's goal is to spread the adoption of cryptocurrencies across global market. We started this year by offering native LTC (Litecoin) processing and launch of API v2. Our next step is to offer payouts in whichever cryptocurrency merchant chooses and no longer be dependent on BTC (Bitcoin) alone. Payouts in LTC should be available to our customers in the upcoming month. This feature will be then expanded by adding different altcoins one-by-one to our portfolio, where we will be able not only to collect various types of altcoins, but make settlements in them as well. Furthermore, we will be able to offer much better exchange rate for the end-customer compared to the current one.*

*Our next target is to start collecting payments over Lightning Network. We hope to deploy it in our sandbox environment within next few weeks for testing and be ready to offer it in production as soon as possible to collect micropayments.*

*Other feature that we will be offering really soon is AML protection for our clients. Currently regulated companies, such as internet gambling, Forex, precious metal etc., have limited accessibility to cryptocurrency as they cannot ensure, that AML and CTF (Counter Terrorist Financing) standards are met. By eliminating ML (Money Laundry) and TF (Terrorist Financing) risks we will open a door for crypto to enter those markets."*

*- Justas Paulius*

As I understand, Coingate plans to put higher priority on finding solutions for the weaknesses of the blockchain to improve the overall satisfaction of everyday users, and to make it more attractive to the general public.

The bottleneck of the blockchain was originally the pre-configured block size, and closing frequency, which had a negative impact on the performance of the network after gaining

media attention in the last few years. The original idea of the Lightning Network was first published by Joseph Poon and Thaddeus Dryja, who have been looking for a solution exactly for the bitcoin scalability problem. It is basically a second layer network on the blockchain specialized in fast and cheap micropayment processing.

Adding native litecoin and later other alternative cryptocurrency processing and payout solutions to the portfolio of Coingate is also an attempt showing the focus on cost optimization. Elimination bitcoin as an intermediary currency, and being able to convert directly into litecoin or other altcoins will improve the general costs of processing for merchants.

Finally fighting the bad reputation of the blockchain originating from terrorism funding and money laundry will help expanding the group of potential industries and as a consequence it will increase the number of cryptocurrency users worldwide.

# Chapter 8. - Summary

All in all blockchain is a smart solution with a huge potential in it, but its users must be careful as it has also countless risk factors. For the time being it has its exact role in the World, which is providing payment solutions for people favorizing anonymity in banking (or trying to avoid involvement of third parties in the payment flow), but I believe there is a chance, that it will be more than that on the medium run.

It offers already a groundbreaking technology, which was able to gain attention of commercial and central banks, and with the new possibilities created by the PSD2, I can foresee, that it can develop in a direction, that it will offer all the advantages of the preferred payment methods like credit card, bank transfers and mobile payments.

Cashless world is the future, therefore financial institution will have to prepare for it, whether they like it or not. But the question is, what kind of cashless solution will be the generally accepted one, if there will be any.

There are already available examples on the market, that offer similar services to the blockchain within the PSD2 framework, and the number of such companies (PISPs and AISPs) will most probably keep on increasing constantly over time, which I am sure will produce innovative solutions on the short run.

But what I have not seen yet is a hybrid combination of blockchain based technologies and PISPs within a regulated framework, which I believe, might be a gamechanger in the status quo.

# Chapter 9. - Conclusion: will the bitcoin and the blockchain survive?

Despite the media attention and its support of innovation, I believe bitcoin is more of a stock-like asset, than an international currency: it is too much volatile mainly driven by speculation.

In my eyes bitcoin is just a pilot project of the blockchain technology with two major features: it can provide “anonymity” in a certain way, and eliminates the need of intermediary parties in the payment flow. But while national currencies are liabilities of the issuing countries’ governments with their central banks protecting and controlling their value, bitcoin is a liability of nobody being controlled also by nobody.

Of course, countries could issue their own cryptocurrencies, and we have seen such initiatives by Russia, Iran, Turkey or Venezuela, but I am not 100% sure, that it would be in the interest of other countries. While bitcoin is still often used for money laundry, tax evasion or terrorism funding, these are all against the interest of any countries in the World. To avoid these risks, national cryptocurrencies must lose anonymity to make them easier to control, but that would kill the number one objective of bitcoin, therefore people would have no interest in changing from bitcoin for example to it.

For this reason I believe bitcoin will keep its role in the economy as it is today, with high chances that it will be dominated by other cryptocurrencies from time to time, but the blockchain technology will set the ground for further innovation in the bank sector.

Thank you for the attention!
David Biczok

# Chapter 10. - References, sources, appendices and acknowledgments

*Egri Szilvia,* 5 January 2018, "Bevezető a Kriptovaluták És a Blockchain Titokzatos Világába", https://fintechzone.hu/bevezeto-kriptovalutak-es-blockchain-titokzatos-vilagaba/

*Cara McGoogan and Matthew Field,* 8 March 2018, "What is cryptocurrency, how does it work and why do we use it?" https://www.telegraph.co.uk/technology/0/cryptocurrency/

*European Payments Council AISBL,* 2017 "SEPA Instant Credit Transfer" https://www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer

*Everest Group,* 11 May 2016, "Defining Blockchain", https://www.everestgrp.com/2016-05-blockchain-technology-bfsi-benefits-market-insights-20805.html/

*Rob Price,* 28 November 2017, "Someone in 2010 bought 2 pizzas with 10,000 bitcoins - which today would be worth $100 million" http://uk.businessinsider.com/bitcoin-pizza-10000-100-million-2017-11?r=UK&IR=T

*Bernard Marr,* 6 December 2017, "A short history of bitcoin and crypto currency everyone should read", https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/2/#1150a7d0533c

*Bitcoin 2040,* 30 September 2017, "A historical look at the price of bitcoin", http://www.bitcoin2040.com/bitcoin-price-history/

*Jake Adelstein,* Nathalie-Kyoto Stucky, 19 May 2016, "Behind the biggest bitcoin heist in history: inside the implosion of Mt. Gox", https://www.thedailybeast.com/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox

*Antonio Madeira,* 28 February 2018, "How does an ICO work", https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/

*Christoph Jehle,* 10 March 2018 "Blockchain: Die Technik, die nicht vergessen kann", https://www.heise.de/tp/features/Blockchain-Die-Technik-die-nicht-vergessen-kann-3986173.html

*Jordan Tuwiner,* 2015, "Is bitcoin anonymous?" https://www.buybitcoinworldwide.com/anonymity/

*Jon Matonis,* 23 June 2013, "Bitcoin Foundation receives cease and desist order from California", https://www.forbes.com/sites/jonmatonis/2013/06/23/bitcoin-foundation-receives-cease-and-desist-order-from-california/#30d7d939518c

*Neil Gandal, JT Hamrick, Tyler Moore, Tali Oberman*, 2017, "Price manipulation in the bitcoin ecosystem" http://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_21.pdf

*Nate Raymond,* 5 February 2015, "Accused Silk Road operator convicted on U.S. drug charges", https://www.reuters.com/article/us-usa-bitcoin-trial/accused-silk-road-operator-convicted-on-u-s-drug-charges-idUSKBN0L82H920150205

*Bitcoin-made-easy,* 2018, "About Bitcoin" https://bitcoin-made-easy.com/about-bitcoin/?ccce=cart&a=add&domain=register&PageSpeed=noscript

*Paolo Tasca, Shaowen Liu , Adam S. Hayes,* 1 July 2016, "The Evolution of the Bitcoin Economy: Extracting and Analyzing the Network of Payment relationships", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762

*Coindesk,* 2018, "Bitcoin (USD) Price", https://www.coindesk.com/price/

*Sara Hsu,* 15 January 2018, "China's shutdown of bitcoin miners isn't just about electricity", https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-shutdown-of-bitcoin-miners-isnt-just-about-electricity/#728df844369b

*Nathaniel Popper,* 27 October 2017, "An explanation of the initial coin offerings",

https://www.nytimes.com/2017/10/27/technology/what-is-an-initial-coin-offering.html

*Nathaniel Popper,* 6 November 2017, "Hedge funds push up the price of bitcoin to new highs", https://www.nytimes.com/2017/11/06/technology/bitcoin-hedge-funds.html?rref=collection%2Fbyline%2Fnathaniel-popper

*Jackie Wattles,* 10 December 2017, "Bitcoin jumps after futures trading begins", http://money.cnn.com/2017/12/10/technology/bitcoin-futures-trading/index.html

*Chuck Jones,* 12 March 2018, "Blaming Mt. Gox For Bitcoin's Recent Price Drop Just Doesn't Compute", https://www.forbes.com/sites/chuckjones/2018/03/12/blaming-mt-gox-for-bitcoins-recent-price-drop-just-doesnt-compute/#600e2ee17d61

*Portfolio.hu,* 5 December 2017,"Itt vannak a világ első bitcoinmilliárdosai", https://www.portfolio.hu/vallalatok/itt-vannak-a-vilag-elso-bitcoinmilliardosai.270067.html

*Allan Eberhart,* 6 April 2017, "SEC Rejects Bitcoin ETFs: Should You Reject Bitcoin Investments?", https://www.forbes.com/sites/allaneberhart/2017/04/06/sec-rejects-bitcoin-etfs-should-you-reject-bitcoin-investments/#6228f25379bd

*Thomas Franck,* 20 December 2017, "NYSE files to list bitcoin ETFs, bringing cryptocurrency a step closer to mainstream", https://www.cnbc.com/2017/12/20/nyse-files-to-list-bitcoin-etfs-bringing-cryptocurrency-a-step-closer-to-mainstream.html

*Sumit Roy,* 21 December 2017, "Top performing ETFs of the year", http://www.etf.com/sections/features-and-news/top-performing-etfs-year

*Rilcoinblog,* 8 September 2017, "10 Coins that crossed 1 Billion USD", https://rilcoinblog.com/2017/09/08/10-coins-that-crossed-1-billion-usd/

*Admiral Markets,* 2018, "Mi a Bitcoin Cash?", https://admiralmarkets.hu/education/articles/trading-instruments/mi-a-bitcoin-cash

*Unknown author*, 8 February 2018, "What is Ethereum", https://www.finder.com/ethereum

*Unknown author,* 8 February 2018, "What is Ripple", https://www.finder.com/ripple

*Unknown author,* 8 February 2018, "What is Litecoin", https://www.finder.com/litecoin

*Unknown author,* 8 February 2018, "What is Neo", https://www.finder.com/neo

*Trustnodes, 22 November 2017,* "Ethereum now handles more transactions than all digital currencies combined", https://www.trustnodes.com/2017/11/22/ethereum-now-handles-transactions-digital-currencies-combined

*Bitinfocharts, 18 March 2018,* "Cryptocurrency charts", https://bitinfocharts.com/cryptocurrency-charts.html

*Farkas Dezső,* 19 November 2017, "Hogyan született a Bitcoin, avagy a kriptovaluta és a blockchain rejtélyes világa", http://jovotepitok.hu/hogyan-szuletett-bitcoin-avagy-kriptovaluta-es-blockchain-rejtelyes-vilaga/

*Adam Badenhorst,* 10 December 2017, "Risks in an unregulated crypto market", https://currencies101.com/risks-unregulated-crypto-market/

*Patrick Thompson,* 24 February 2018, "Pump and Dump in Crypto: Cases, Measures, Warnings", https://cointelegraph.com/news/pump-and-dump-in-crypto-cases-measures-warnings

*William Restis,* 19 February 2018, "Whistleblower Awards From Cryptocurrency Pump and Dump Schemes", https://restislaw.com/cftc-crypto-pump-dump-whistleblower/

*Kapersky Lab,* 18 August 2017, "Six myths about the blockchain and Bitcoin: Debunking the effectiveness of the technology", https://www.kaspersky.com/blog/bitcoin-blockchain-issues/18019/

*Blockchain Luxembourg S.A.R.L.,* 9 April 2018, "Hashrate Distribution", https://blockchain.info/pools

*Jamie Burke*, April 2017, "ICO Pros & Cons: Cutting Through The Hype",

https://outlierventures.io/research/cutting-through-the-ico-hype/

*Adam Rogers,* 15 December 2017, "The hard math behind Bitcoin's global warming problem", https://www.wired.com/story/bitcoin-global-warming/

*Julian Mitchell,* 15 December 2016, "Meet The 27-Year-Old Mathematician Building A Bitcoin Empire", https://www.forbes.com/sites/julianmitchell/2016/12/15/meet-the-27-year-old-mathemetician-building-a-bitcoin-empire/#2b960afd1d74

*Digiconomist,* 11 April 2018, "Bitcoin Energy Consumption Index", https://digiconomist.net/bitcoin-energy-consumption

*Jay Adkisson,* 9 February 2018, "Why Bitcoin Is So Volatile", https://www.forbes.com/sites/jayadkisson/2018/02/09/why-bitcoin-is-so-volatile/2/#164c9b6790de

*David Drake,* 2 March 2018, "What is making bitcoin so volatile?", https://irishtechnews.ie/what-is-making-bitcoin-so-volatile-insights-with-david-drake/

*Jean-Paul Rodrigue,* 2017, "The geography of transport systems", https://transportgeography.org/?page_id=9035

*Laura He,* 11 April 2018, "Demand from institutional investors drives up bitcoin futures trading volumes on CME", http://www.scmp.com/business/markets/article/2141119/demand-institutional-investors-drives-bitcoin-futures-trading

*Alexander Kravets,* 18 January 2018, "Institutional Investors Will Bet Big on Cryptocurrencies in 2018", https://cointelegraph.com/news/institutional-investors-will-bet-big-on-cryptocurrencies-in-2018

*Jordan Tuwiner,* 2018, "Bitcoin Anonymity - Is Bitcoin Anonymous?", https://www.buybitcoinworldwide.com/anonymity/

*Matthew Sparkes,* 23 January 2015, "The £625m lost forever - the phenomenon of disappearing Bitcoins", https://www.telegraph.co.uk/technology/news/11362827/The-625m-lost-forever-the-phenomenon-of-disappearing-Bitcoins.html

*Olga Kharif,* 18 January 2018, "Hackers Have Walked Off With About 14% of Big Digital Currencies", https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies

*Kai Sedgwick,* 10 December 2017, "Despite What Politicians Say — Terrorists Don't Use Bitcoin", https://news.bitcoin.com/despite-politicians-say-terrorists-dont-use-bitcoin/

*C. Edward Kelso,* 2 March 2018, "EU Losing Patience – Urges Global Crypto Regulation", https://news.bitcoin.com/eu-losing-patience-bitcoin-needs-global-regulation/

*Buy Bitcoin Online,* 3 May 2018, "The Bitcoin Volatility Index", https://www.buybitcoinworldwide.com/volatility-index/

*Sudhir Khatwani,* 29 March 2018, "Bitcoin Private Keys: Everything You Need To Know", https://coinsutra.com/bitcoin-private-key/

*European Parliament and European Council,* 13 November 2007, "Pénzforgalmi szolgáltatások az EU-ban", http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:l33226&from=EN&isLegissum=true

*Payments, Cards and Mobile*, 18 May 2016, ,"Opportunities unlocked by revised PSD2", http://www.paymentscardsandmobile.com/wp-content/uploads/2016/05/Final-Accenture-Payment-Services-PSD2-PoV-Web-April-2016.pdf

*HSBC*, 2018, "Payment Services Directive II (PSD2)", http://www.gbm.hsbc.com/-/media/gbm/reports/insights/payment-services-directive-ii-psd2.pdf

*HSBC*, 2018, "Payment Services Directive II (PSD2)",http://www.gbm.hsbc.com/insights/technology/payment-services-directive-ii-psd2

*Nemeth Monika,* 19. March 2018, "2019 márciusától elérhető lesz az összes banki API az EU-ban", https://fintechzone.hu/psd2-banki-api-2019/

*Charles Fogg, Bige Ltd.,* 8 May 2018, “Bige Closed loop processing”
http://www.bigeltd.com/wp-content/uploads/2018/04/closed-loop-processing.png