Bitcoin - An Introduction to Risky Money

CHALMERS UNIVERSITY OF TECHNOLOGY

Financial Risk MVE220

Abstract

This report is intended to provide information about Bitcoin, its risks and potentials for the future. It first gives a basic overview of the technical principle of Bitcoin and the Blockchain technology. Different security mechanisms of Bitcoin are explained. Based on this, the report presents some major risks and limitations of Bitcoin. Finally, the report discusses whether Bitcoin has a potential to replace conventional currencies and serve as an everyday life means of payment in the future.

Autor: Michael Socha

Course Instructor: Professor Holger Rootzen

A.Y. 2018-2019

Spring Semester

Table of Contents

1 Introduction

During the financial crisis of 2008, when many people had lost confidence in banks, a pseudonymous software developer named Satoshi Nakamoto published a white paper on an electronic peer-to-peer payment system that can operate entirely without any central authority such as a bank (Nakamoto 2008). In 2009, Bitcoin was established. Only after a short time, interest in this newly developed crypto currency grew. More and more investors sensed good chances for high increases in value. At first, they seemed to be on the right track: within eight years, the Bitcoin value rose from less than one U.S. penny to almost USD 20,000 (Kumar, Smith 2018). After a downward slide in 2018, however, the value of Bitcoin today only fluctuates by around USD 5,000. Nevertheless, "the original" among the crypto currencies remains the world's most popular e-currency, with a market capitalization of around USD 110 billion (blockchain.com 2019).

Bitcoin is very complex. It is based on an advanced technological-mathematical foundation whose basic understanding is a prerequisite for making serious investment decisions or forming an opinion. In the past, arguments about Bitcoin were often characterized by euphoria and possible risks were not always considered very intensively. This report therefore aims to provide information on Bitcoin and its risks. The first part of this report will give a fundamental overview of how Bitcoin works. In a second part, risks of Bitcoin will be introduced. Finally, a brief discussion will be given on the future suitability of Bitcoin as an everyday life means of payment.

2 The Mechanisms of Bitcoin and Blockchain

Against the backdrop of the financial crisis in 2008, Satoshi Nakamoto intended one thing above all with his Bitcoin: to establish a currency system that people can trust on, where no bank services from third parties are required anymore (Nakamoto 2008). Nakamoto's Bitcoin is therefore based on a decentralised peer-to-peer system in which Bitcoin users themselves take on central banking functions. If, for example, a user wishes to carry out a transaction, a general consensus must first be reached on the legality of this transaction throughout the Bitcoin network before it can be authorized (Böhme et al. 2015). But how can such a general consensus be reached? And how does the Blockchain technology relate to this? These questions will be discussed in the following sections of Chapter 2. Readers less interested in the technical details of Bitcoin could skip to chapter 3.

2.1 The Functioning of a Blockchain

Bitcoin is based on the blockchain technology. Blockchains are used in many contexts, often when data needs to be encrypted and documented, such as passwords, contracts or, in the case of Bitcoin, financial transactions. A blockchain is a sequence of data packages that is constantly updated and extended by new data packages/blocks. In the case of the Bitcoin blockchain, the blocks contain transaction data (Kumar, Smith 2018).

Fundamental for a blockchain is a cryptographic encryption mechanism for data, a so-called hashing algorithm. Bitcoin uses the SHA-256 algorithm. This algorithm converts any letter, number sequence or text of any length (input) into a 64-digit long code, a so-called hash value (output) (Narayanan et al. 2016). The hash value of the words "Financial Risk" for example is "1258883ba66afcfdfdf7b815bde64655fa1764b376654ef2674a2cda80cfc763a0" (check it on anders.com 2018). The generation of a new hash value is unpredictable, and every change of the input data leads to a strongly changed hash value. Exactly identical inputs, however, always generate the same hashes (Narayanan et al. 2016). Based on the hash value, the original data input cannot be determined with reasonable effort (Franco 2015).

By looking at the Bitcoin blockchain (two consecutive blocks n and n+1 are shown as examples in Figure 1), it becomes visible that each individual block of the chain contains data (transaction data and a previous hash). Then each block also contains a hash value. These hash values are the outputs of the SHA-256 algorithm for the input that is listed in each data field. For reasons of clarity, the hash value in this example has been reduced to only eight characters.

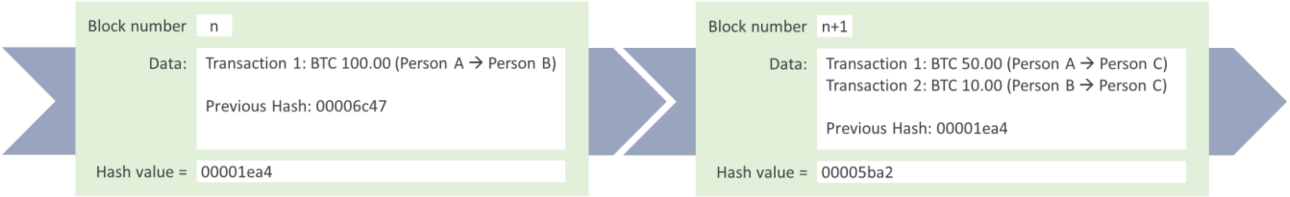
Block number n
Data: Transaction 1: BTC 100.00 (Person A → Person B)
Previous Hash: 00006c47
Hash value = 00001ea4
Block number n+1
Data: Transaction 1: BTC 50.00 (Person A → Person C)
Transaction 2: BTC 10.00 (Person B → Person C)
Previous Hash: 00001ea4
Hash value = 00005ba2

Figure 1 Example of two Bitcoin blockchain blocks filled with transaction data (inspired by Brownworth 2017)

Thus, in a block n+1 of a blockchain, the hash of this block gets influenced not only by the transaction data n+1, but also by the previous hash, the hash of block n. For a previous hash listed in the data field of block n+1, it applies that this hash does not represent a static hardcopy of hash n, but in the case of an update of block n's hash value, hash n+1 would synchronize with the updated version of hash value n. This is the reason why blockchains are considered to be very safe with regard to manipulation, because if block n was manipulated, not only his hash would change, but also all hashes of the following blocks n+m. The manipulated block n would be immediately identifiable (Brownworth 2017).

2.2 Bitcoin Explained Using the Example of a Transaction

In a Bitcoin blockchain, only transaction data is stored, no account balances. However, account balances can easily be calculated as the difference between all transactions of a user (Antonopoulos 2014). Since the Bitcoin blockchain is based on transaction data, the best way to explain Bitcoin's principles is to use a transaction as an example.

If user A wants to transfer an amount of money to user B, both need a so-called wallet - software, which can be downloaded for the smartphone or the computer. When user A releases his/her transaction, it is first added to a "memory pool" where it is waiting together with other unconfirmed transactions of other users for verification (Saad et al 2019).

In the following, so-called "Miners" come into play. Miners are essentially accountants who are required to ensure the correctness of all Bitcoin transactions. In principle, any Bitcoin user can act as a Miner, but there is no obligation to do so. If a user participates in mining, he/she can be described as an active user; users who abstain from mining can be described as passive users. A transaction is valid when the majority of all Miners agree to its correctness (peer to peer principle). One estimate from late 2015 suggested that there were around 100,000 Miners (Kumar, Smith 2018).

First, each Miner selects various transactions from the memory pool. It is up to each Miner to decide which and how many transactions to select. On average, a Miner chooses more than 500 transactions (Cosset 2017). Once a Miner has made his selection, he inserts his transaction data into the SHA-256 algorithm together with the hash of the current block of the Bitcoin blockchain and generates a new hash value (Brownworth 2017).

Now, a Miner must prove to the entire network of Miners that the transactions he has selected are correct and that he has not manipulated them in his favor. In the case of Bitcoin, this is done by using a "Proof of Work" approach. This means that each Miner has to solve a calculation intensive problem. In case they find a correct solution, this solution is recognized as a proof that their selected transaction data is unmanipulated and correct (Kumar, Smith 2018).

Within Proof of Work, a Miner must manipulate his computed hash value so that it becomes smaller than a target value given by the Bitcoin system (Narayanan et al. 2016). In order to modify the appearance of hashes without changing the input data itself, SHA-256 offers the possibility to insert a so called nonce, a 16-bit character string as a further input. Entering and changing a nonce also changes the hash value (unpredictably). A Miner has to try so many nonces until he randomly finds a nonce value that changes his hash value in the desired way. In practice, this is extremely computation intensive. Miners must perform billions of operations per second to solve such nonce-hash puzzles (Böhme et al. 2015). Therefore, Miners need huge amounts of computation power (hashing power).

The Miner who first finds a correct nonce shares it with the community, along with his updated nonce-influenced hash value and his selected transactions. The other Miners verify the results by inserting the nonce and the transaction data into the SHA-256 algorithm and calculating the corresponding hash value. If their hash values and the hash value of the fastest Miner match, the selected transactions of the fastest Miner will be recognized as valid and appended to the blockchain as a block. In reality, about 10 minutes elapse between the appending of two blocks (Berentsen, Schär 2018).

Miners receive a fee in Bitcoin for their commitment and their provision of computing power. This fee was BTC 12.5 per mined block in 2019 and is halved every 210,000 blocks (approximately every four years) Mining is the only way new Bitcoins can get in circulation. The maximum amount of Bitcoins is limited to BTC 21 million. This threshold is important because it makes Bitcoin a rare commodity, which is a prerequisite for any currency (Berentsen, Schär 2018).

2.3 The Safety Principle of Bitcoin

Essentially, there are three central security mechanisms to ensure security in the Bitcoin network:

Structure of the blockchain:
As already mentioned in chapter 2.1, the blockchain technology with its linking of predecessor hash values enables an immediate identifiability of manipulation. This makes blockchains very secure over long time periods. The Bitcoin blockchain is in existence since 2009. All transactions that have occurred since then are transparent and can be traced with the click of a mouse, making life difficult for criminals, money launderers and fraudsters (Narayanan et al. 2016).

Decentralized storage of the blockchain:
The blockchain transaction data is stored decentral. This means that not one blockchain version is stored on a central server of a party, but many identical versions are stored decentral on nodes (Böhme et al. 2015). Nodes can be all electronic devices that have access to the Internet. Servers of Miners, for example, are nodes (Kumar, Smith 2018). Each time a new block is encoded, it is appended to all copies of the blockchain. If one chain is manipulated, the other chains will not be affected, and manipulations can be immediately detected by chain comparisons (Brownworth 2017).

Proof of Work approach:

Solving the nonce-hash puzzle as part of the Proof of Work approach serves to raise the hurdles for manipulators as high as possible. Fraudsters would first need to gain a significantly higher hashing power than average Miners in order to manipulate transaction data with a realistic probability. This is considered unlikely due to the high expenditure required to purchase the corresponding hardware (Saad et al 2019).

3 Risks of Bitcoin

Every currency holds risks. However, with Bitcoin's merger of two previously separate industries - finance and IT - new, so far irrelevant risks emerge. In the following chapter, five central fields of risks relating to users, investors, the society and the environment will be presented and discussed.

3.1 Volatility Risks

Bitcoin and cryptocurrencies in general undergo strong price fluctuations. In past few years some people have become millionaires overnight as the value increased. However, some people have lost too as the value dropped drastically. The following figure 2 shows the fluctuations of the Bitcoin market price since 2009 in U.S. Dollar.

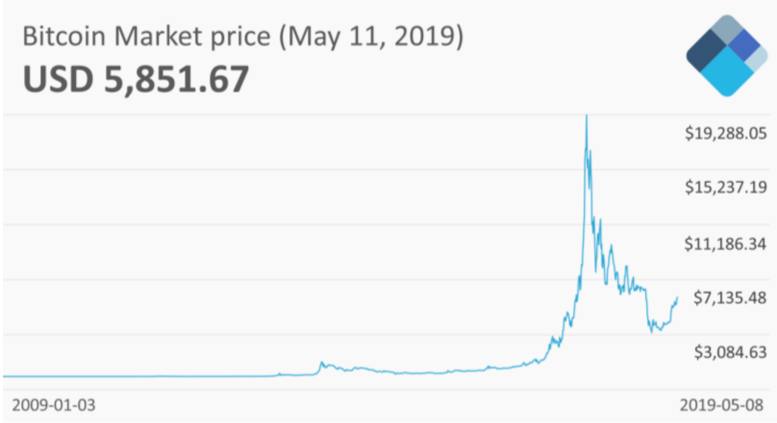

Figure 2 Price of Bitcoin in U.S. Dollar (blockchain.com 2019)

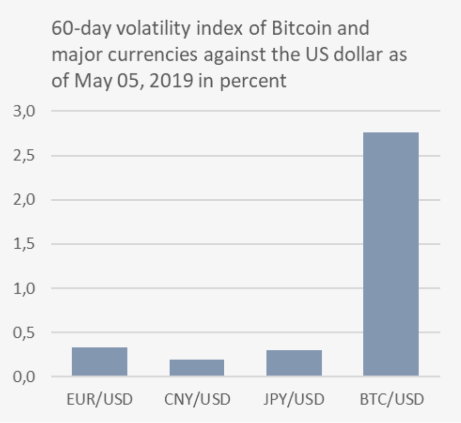

Figure 3 60-day volatility indices of Bitcoin and major currencies (buybitcoinworldwide.com 2019)

In the beginning, when Bitcoin was not so popular, the price remained relatively stable at a low level. Then, in 2017, the currency increased its value to around USD 19,000 but fell sharply shortly thereafter. The exchange rate almost dropped below USD 3,000. There are no clear reasons for this sharp fall in prices. According to experts, a significant impulse was a threat from a South Korean regulatory authority to close the crypto exchanges (Wheatley et al. 2018). In 2019, the price trend was slightly more stable and has been able to increase again recently.

A frequently used risk indicator for investors is volatility - a measure of price fluctuations. The higher the volatility, the stronger the price fluctuation and the riskier an investment (buybitcoinworldwide.com 2019). Figure 3 shows the 60-day volatility index of Bitcoin compared to and other major currencies against the U.S. Dollar as of May 05, 2019. The volatility of Bitcoin is significantly higher than the volatilities of other major currencies. Bitcoin proponents argue that the Bitcoin volatility should decrease to a lower level over time because the currency needs time to establish (Yermack 2018). However, this has not yet happened. In fact, volatility at the end of 2018 had risen to a level not reached since 2015 (buybitcoinworldwide.com 2019).

Bitcoin is extremely volatile. Currently it is only suitable for short-term investments and venture investors. (Yermack 2018). In addition, there are many external factors that influence Bitcoin's value. Much of these factors are of a technical nature and difficult for normal investors to understand or grasp. For instance, which average investor is able to predict such influences like those that might emerge by the upcoming quantum computing, which could have the potential to crack hashes and find nonces ultra-fast one day and thus destroy the Proof of Work mechanism (Xu 2016)?

3.2 Individual Risks - Loss of Private Key

In conventional central monetary systems, users normally do not need to worry about the safekeeping of their money because it is safely stored in a bank vault. In the event of a robbery, the customer is insured. Unintentional transactions can also be reversed by banks. In Bitcoin, however, the user himself is responsible for the safekeeping and the security of his monies. Bitcoin holders store their coins in digital wallets. A user has access to the wallet via a private key. If this key gets lost, everyone who owns it has access to the Bitcoins it contains (Böhme et al. 2015). Private keys can be lost in many ways: by phishing, hacking, malware, or simply misplacing or forgetting (Weaver 2018).

According to estimates by the digital forensics company Chainalysis, about BTC 3 million had finally gone for good by 2017. These figures imply 17% to 23% of all existing Bitcoins from 2017 (Roberts, Rapp 2017) and would be worth USD 15.00 billion by May 2019 (blockchain.com, 2019).

There are numerous horror stories of Bitcoin owners committing careless key management and losing millions of dollars in the course of it. For example, a Briton who, while cleaning up his desk, simply threw away an old hard drive with BTC 7,500 (worth about USD 37 million according to today's exchange rate) or USB sticks with thousands of Bitcoins stored on that simply broke (Pollock 2017). For Bitcoin owners it is therefore essential to take care of private keys and take all possible security precautions, such as working in secure networks or installing anti-virus software.

3.3 Systemic Risks - Majority Attack

The most central risk intuitively associated with digital currencies is certainly hacking. Systemic attacks, i.e. attacks on the overall system (Weaver 2018) and not on the user's wallet, are particularly worrying because even the best protected users cannot protect themselves against such attacks. One of the most popular of such risks is the Majority Attack, also referred to as 51% attack.

A 51% attack always proceeds from a malicious Miner. The prerequisite for such an attack is that a criminal Miner manages to bundle more than 51% of the total computing power of the entire Bitcoin network. This gives him an absolute majority and puts him in the position of being able to insert fraudulent transactions into the blockchain, and as a consequence to double spend money or steal assets from other Bitcoin users (Nakamoto 2008; Xu 2016; Saad 2019).

Realistically, a majority attacker is only able to manipulate transactions within the last few blocks. The longer a transaction is back in time, the better protected it is (learncryptography.com 2019) For a payee, this means that the more time has passed since the payment was received, the greater the probability that manipulation can be excluded. As a rule, a payee can consider a transaction secure and confirmed after about seven blocks, which corresponds to about 70 minutes of waiting time (Narayanan et al. 2016).

The majority attack is so interesting because it represents a weak point of every public block chain. As soon as a user has sufficient computing power, there is no authority that could prevent him from carrying out such an attack. Prevention is practically impossible (learncryptography.com 2019). So far, no majority attack has been carried out on Bitcoin, and the risk is considered low, as hackers would need to pool a great deal of computing power to overcome Bitcoin's network. Currently not even large-scale governments are able to accomplish this (learncryptography.com 2019). At the moment, blockchains with a smaller and younger network are more endangered (Xu 2016). For example, only in January 2019 an attack was carried out on Ethereum Classic, the 18th largest crypto currency by market cap, with estimated losses of USD 1.1 million (Lielacher 2019).

However, with the increasing number of shared mining offerings - a type of cloud mining where multiple users share computing power for mining - the risk of a Majority Attack on Bitcoin increases as shared computing makes it easier and more affordable to gain the hashing power needed (learncryptography.com, 2019). In March 2015, the two largest mining pools, AntPool and F2Pool, accounted for about one third of all mining activity at the time (Böhme et al. 2015). The risk of a Majority Attack is therefore present and should not be underestimated, especially for smaller crypto currencies or in phases when Bitcoin is losing popularity.

3.4 Risks to Society - Cyber Assisted Crime

The risks mentioned so far are limited to the users of cryptocurrencies. But in Bitcoin and in cryptocurrencies in general there is also a great risk for society as a whole, because cryptocurrencies offer a new breeding ground for criminals and fraudsters and are very suitable for money laundering.

Cryptocurrencies make criminal money transactions immensely easier because transactions can be concealed. While Bitcoin is very transparent - each transaction is recorded in the blockchain - the transaction data is not directly linked to names, physical addresses or other identifying information, which makes digital currencies to some extent anonymous and difficult for law enforcement agencies to identify individual transactions and connect them to users (van Wegberg, Oerlemans, van Deventer 2018).

According to a study conducted by Europol in 2015, about 40% of all identified criminal-to-criminal payments were processed via Bitcoin (Europol 2015). Above all, Bitcoin has become the number one payment method in darknet marketplaces (online marketplaces connecting buyers with sellers of illicit goods and services, such as drugs or guns) and has helped these markets to achieve great upswings (Fanusie, Robinson 2018). Bitcoin also plays a role in terrorist organizations: in 2014, reports appeared about fighters of the Islamic state terrorist organization (IS) in Syria who made purchases and conducted international transactions with digital currencies such as Bitcoin. In 2017, a woman was arrested in New York for transferring USD 62,000 in Bitcoin to the IS (Malik 2018).

But not only do Bitcoin or cryptocurrencies make money transfers easier for criminals and terrorists - their anonymity is also perfect for money laundering. For this, criminals and fraudsters convert their illegally acquired money into Bitcoin (or acquire it already in Bitcoin, as in some 90 percent of all cases) and then let it pass through conversion services to disguise the origin of their dirty money (Fanusie, Robinson 2018). The most popular conversion services are Bitcoin exchange services, online gambling or Bitcoin-mixing (an online software service that makes the Bitcoin transaction history unrecognizable). A 2018 study estimates that the amount of Bitcoin that passed through conversion services between 2013 and 2016 is about 0.61 percent of the total Bitcoin inventory (Fanusie, Robinson 2018). However, due to the complicated data collection situation, this number can only be regarded as an estimate and is to be interpreted as a minimum threshold. The true percentage of Bitcoin laundering is likely to be higher (Fanusie, Robinson 2018).

Experts assume that money laundering in cryptocurrencies could become more attractive in the future, especially if cryptocurrencies were to establish as a general means of payment, since after money laundering no complicated exchanges into conventional currencies would then be required any longer (Weaver 2018).

3.5 Risks for the Environment

Mining, solving the mathematical puzzle to find a nonce, requires enormous amounts of energy. Current estimates assume that in 2019 about 60 Terra Watt hours (TWh) of energy will be used for Bitcoin Mining. At the moment, one Bitcoin transaction alone could supply 14 U.S. households with energy for a single day. One transaction causes a carbon footprint of 206.1 kg of CO2. In a recent study, experts estimate that all Bitcoin transactions combined will consume as much electricity in 2020 as Denmark (digiconomist.net 2019). This high energy consumption is a cause of great concern for environmentalists because most mining energy is unlikely to come from renewable sources, considering the global energy mix. In China, for example, which leads Bitcoin mining, 60% of energy comes from coal (Lou 2019).

In light of this high energy consumption, the question arises whether there are any other mechanisms in place of Proof of Work, that are able to provide security in the Bitcoin network. In fact, there are several alternatives, some of which are already being tested on other crypto currencies. Currently, Etherium, the second largest crypto currency in terms of market capitalization, is planning a transition from Proof of Work to a Proof of Stake approach, where those Miners are responsible for validating transactions that deposit the largest amount of coins (Lisk Foundation 2019).

Whether such an approach can be equally secure remains to be seen. However, proof of work cannot be the solution if Bitcoin wants to be morally justifiable in the future. Against the background of climate change, new innovations should not contribute to further worsening the global climate balance. Especially not in a way that has no value for society, as is the case with the solving of nonce-hash puzzles.

4 Bitcoin as Future Everyday Life Currency?

Given Bitcoin's high popularity, it is interesting to examine whether Bitcoin has the potential to establish as an everyday life currency one day and replace traditional state related currencies. From an economic point of view, our everyday life money is typically characterized as having three major attributes: "It serves as a medium of exchange, a unit of account, and a store of value" (Yermack 2018). How well does Bitcoin meet these attributes?

As a medium of exchange, Bitcoin is not yet particularly well established worldwide. In 2016, only about 106,000 businesses accepted Bitcoin (Weber, 2016 01). However, influential online shipping companies such as Amazon could significantly boost the popularity of Bitcoin if they would decide to accept the crypto currency one day. Bitcoin is also not very suitable as a unit of account. Its volatility makes daily purchases confusing and incomparable. How can one do everyday businesses quickly and easily when prices are exposed to permanent massive fluctuations? As a store of value, Bitcoin is subject to great challenges from constant dangers of cyber crime, fraud, technical innovation and bubble formation due to euphoric investment runs. Against this backdrop, Bitcoin cannot be considered a safe store of value.

Under the given circumstances, Bitcoin cannot be regarded as a suitable everyday life means of payment. It does not meet any of the three characteristic criteria very well. But what if Bitcoin was to be further developed, say into a kind of mixture between Bitcoin and conventional currencies, in which the democratic but poorly regulable participation principle of mining would be abandoned to a certain extent and instead replaced by a central administration who would take on the tasks of validating transactions and updating the blockchain? Indeed, there are some scientific discussions about such centralized constructs (Yermack 2018). Centralized cryptocurrency models may have the potential to address the challenges and risks that Bitcoin is faced with:

For example, in centralized blockchain models, the volatility could likely be reduced because a central administration could intervene in regulation and, for instance, limit the access for venture speculators. Also, cyber assisted crime, money laundering and darknet businesses could be mitigated, with the central administration having access to the names behind the transaction data and thus being able to easily track down suspects. Additionally, the risk of a majority attack could be completely ruled out without Miners validating transactions. Furthermore, the risk of losing private keys could be eliminated because a central administration would be able to restore accounts or issue new credentials upon a proof of identity of an affected user. Finally, the environmental impact could be significantly reduced because energy-intensive mining would no longer be required.

A centralized cryptocurrency would have significant advantages compared to Bitcoin. Due to its centralized regulatory, many risks that Bitcoin is faced with could be reduced. A centralized cryptocurrency would therefore have the potential to become more stable and thus better fit as an everyday life currency.

However, a central administration would have to be trustworthy. For instance, central banks could take on the role of administrators. Also, it would be conceivable for this job to be done by a kind of committee, democratically elected by the users on a regular basis, comparable to the election of a government. A centralized model could become a threat if it was abused by totalitarian regimes by restricting freedoms of citizens and implementing total surveillance.

Bitcoin itself is unlikely to become competitive with other major currencies in terms of everyday life suitability and popularity. Risks are too unpredictable at the moment. However, Bitcoin can serve as a basis for building a more advanced cryptocurrency model. But such a model would have to be a compromise between central control and decentralized freedom. A coexistence of several currency models would be conceivable in the future, whereby users could choose their preferred currency depending on their personal risk tolerance.

5 Conclusion

Bitcoin is a major playing field. Blockchain technology and the principle of Proof of Work are highly complex, and a complete understanding of the technology requires advanced mathematical and programming skills. Risk assessment is difficult because there are many value-influencing parameters. In addition, the consequences of Bitcoin are extensive. They can affect a whole society through crime, money laundering and environmental threats. Currently, Bitcoin or related cryptocurrencies are not suitable as an everyday life means of payment and can be regarded more as an investment vehicle for risk-averse speculators. It remains to be seen how the crypto market will continue to develop.

6 Recommendations for Further Reading

The topic Bitcoin is very popular at the moment and therefore many literature is available. The following literature, however, is highly recommendable due to its good mixture between informativeness and comprehensibility.

About the functionality of Bitcoin and Blockchain it is recommendable to further read:

- Kumar, A., & Smith, C. (2017). Crypto-currencies–An introduction to not-so-funny moneys (No. AN2017/07). Reserve Bank of New Zealand.
- Antonopoulos, A. M. (2014) Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O ´Reilly Media, Sebastopol, CA
- Franco, P. (2015) Understanding Bitcoin: Cryptography, Engineering, and Economics, Wiley, Chichester

In particular, it is highly recommendable to check the following Blockchain demo tool by Anders Brownworth. He explains the principles of Blockchains very comprehensible.

- Brownworth, A. (2017). Blockchain Demo. click here

About risks of Bitcoin and Cryptocurrencies, the following literature is recommendable:

- Weaver, N. (2018). Risks of cryptocurrencies. Communications of the ACM, 61(6), 20-24
- Malik N. (2018). How Criminals And Terrorists Use Cryptocurrency: And How To Stop It. click here

About the future and the potentials of Cryptocurrencies:

- Yermack, D. (2018). The potential of digital currency and blockchains. NBER Reporter, (1), 14-17.

References

Antonopoulos, A. M. (2014) Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O ´Reilly Media, Sebastopol, CA.

Berentsen, Aleksander, and Fabian Schär. "A short introduction to the world of cryptocurrencies." (2018): 1-16.

blockchain.com (2019). Available at: https://www.blockchain.com/ (accessed May,05 2019).

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-38.

Brownworth, A. (2017). Blockchain Demo. Available at: https://anders.com/blockchain/distributed.html (accessed May,11 2019).

buybitcoinworldwide.com (2019). Der Bitcoin-Volatilitätsindex. Available at: https://www.buybitcoinworldwide.com/de/volatilitatsindex (accessed May,05 2019).

Cosset, D. (2017). Blockchain: what is in a block? Available at: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo (accessed May,10 2019).

digiconomist.net (2019). Available at: https://digiconomist.net/bitcoin-energy-consumption (accessed May,10 2019).

Europol, E. C. C. (2014). The Internet Organised Crime Threat Assessment (IOCTA).

Fanusie, Y., & Robinson, T. (2018). Bitcoin laundering: an analysis of illicit flows into digital currency services. Center on Sanctions & Illicit Finance memorandum, January.

Franco, P. (2015) Understanding Bitcoin: Cryptography, Engineering, and Economics, Wiley, Chichester.

Kumar, A., & Smith, C. (2017). Crypto-currencies–An introduction to not-so-funny moneys (No. AN2017/07). Reserve Bank of New Zealand.

learncryptography.com. 51% Attack. Available at: https://learncryptography.com/cryptocurrency/51-attack (accessed May,05 2019).

Lielacher A. (2019). ETC 51 % attack – what happened and how it was stopped. Available at: https://bravenewcoin.com/insights/etc-51-attack-what-happened-and-how-it-was-stoppe (accessed May,11 2019).

Lisk Foundation (2019). Proof of Stake. Available at: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-stake (accessed May,09 2019).

Lou E. (2019). Bitcoin Energy Data. Available at: https://www.theguardian.com/commentisfree/2019/jan/17/bitcoin-big-oil-environment-energy (accessed May,12 2019).

Malik N. (2018). How Criminals And Terrorists Use Cryptocurrency: And How To Stop It. Available at: https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#53bfc81f3990 (accessed May,11 2019).

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.

Pollock, D. (2017). Infamous Discarded Hard Drive Holding 7,500 Bitcoins Would be Worth $80 Million Today. Available at: https://cointelegraph.com/news/infamous-discarded-hard-drive-holding-7500-bitcoins-would-be-worth-80-million-today (accessed May,11 2019).

Roberts J. J., & Rapp N. (2017). Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says. Available at: http://fortune.com/2017/11/25/lost-bitcoins/ (accessed May,11 2019).

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. (2019). Exploring the Attack Surface of Blockchain: A Systematic Overview. arXiv preprint arXiv:1904.03487.

van Wegberg, R., Oerlemans, J. J., & van Deventer, O. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. Journal of Financial Crime, 25(2), 419-435.

Weaver, N. (2018). Risks of cryptocurrencies. Communications of the ACM, 61(6), 20-24.

Wheatley, S., Sornette, D., Huber, T., Reppen, M., & Gantner, R. N. (2018). Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the LPPLS Model. (March 15, 2018). Swiss Finance Institute Research Paper, (18-22).

Xu, J. J. (2016). Are blockchains immune to all malicious attacks? Financial Innovation, 2(1), 25.

Yermack, D. (2018). The potential of digital currency and blockchains. NBER Reporter, (1), 14-17.