Blockchain - The Revolution of Community-based Decentralized Open Ledger Technologies

Markus Schindler, MA
SzéchenyiIstván School of PhD Students
University of Sopron
Kirchfeldgasse 60/4/7
2482 Münchendorf, Austria

Abstract

Cryptocurrencies as applications on the Blockchain and community based decentralized open ledger technologies have been very controversial issues ever since they have come into existence. The underlying technology of cryptocurrencies, the Blockchain, may be an as disrupting technology leap as the invention of the Internet. In simple terms, Blockchain technology is a concatenation of blocks of information – transactions in the case of cryptocurrencies – with certain hashing algorithms using the hash values of previous blocks in the following ones. A copy of the entire Blockchain is stored on each participant's computer. In case any Blockchain copy is manipulated, for example by changing the transactions data, the other participants will notice this manipulation and overwrite the faulty information. Blockchain technology is claimed to be a very secure technology for storing information. The aim of this paper, which is part of the research for my doctoral thesis, is to create a deeper understanding of what the Blockchain actually is and how its technology is capable of changing the way people interact with each other without a centralized trusted third party.

Keywords: Blockchain, Bitcoin, cryptocurriencies, decentralized

1. Bitcoin, Altcoins and the Blockchain

Cryptocurrencies like Bitcoin and Ethereum are experiencing a veritable boom. However, the prevailing opinion among many investors and consumers, is that these digital currencies are only for computer experts, with no potential as a means of transaction or as an investment. Meanwhile, crypto currencies are well known to many, but so far, they are notwidely used. Nevertheless, bitcoin and other digital currencies offer countless possibilities for modern payment, investment or transfers, which at the moment are not used by consumers and investors often.[1]

In simple terms, cryptographic currencies are a kind of digital money. They are especially versatile on the Internet. These currencies, such as Bitcoin, Ethereum, or Dash, to only name a few, are being generated on a blockchain, an infinite code chain that is constantly being solvable, distributed, and converted by different high-performance computers (a process called 'mining'). They can be freely purchased without restriction, in order to make purchases online or to send money worldwide within minutes. In addition, they are traded on the currency market like classic currencies and used by many investors for speculation.[2]

The main difference between cryptocurrencies and fiat money is the regulation, as well as the origin of the money. Traditional money is issued and regulated by a central bank on the basis of investments and debts. By contrast, cryptocurrencies are created as part of the blockchain process. For most cryptocurrencies, the quantity is determined.[3]

The storing of cryptocurrencies is different to ordinary money. Cryptocurrencies exist only on the blockchain in the form of an access code. Since cryptocurrencies are decentralized, they are always owned by the owner of the private key. Usually, cryptocurrencies are kept in so-called wallets, a kind of online access to the Blockchain for managing the digital balance.[4]The price performance of a cryptocurrency is similar to traditional currencies, but it is more volatile and more sensitive to daily news, supply and demand. Anyone who has been closely observing bitcoin development since its beginning is aware of the volatile movements, which has caused the price of the digital currency to ultimately surpass the value of 20.000 Dollar at one point, after a lot of ups and downs.

[1] AndreasAntonopoulos, Mastering Bitcoin: Programming the open Blockchain (Sebastopol: O'Reilly Media, Inc, 2017), 4.
[2] Swan Melanie, Blockchain: Blueprint for a new economy (Sebastopol: O'Reilly Media, Inc., 2017), 2-4.
[3] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 80-4.
[4] Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 5-9.

Generally, as with other currencies, the basic law of supply and demand applies. In addition, an elevated market value often reflects increased investor confidence. Decreasing investor confidence will result in mass selling and a devaluation of the market value - just like a normal currency, only more volatile.[5]

Cryptocurrencies are versatile and in some cases a very attractive alternative to money. With their low transaction costs, they offer both companies and individuals the ability to send money easily and quickly. Because unlike traditional cash, crypto coins do not exist in a specific location, but only as a line of code on the blockchain, they can move from the sender to the recipient within minutes, or in some cases even seconds - a transaction that would take several days and significantly higher costs with an ordinary bank.[6]

The area of cryptocurrencies is still very young and somewhat volatile. Because digital currencies are not regulated, their price performance is even more unpredictable than that of a common currency or stock. For example, if an investor chooses to sell a cryptocurrency in bulk, it has an even greater devaluation effect than it would have on a common currency.[7]

2. A brief description of cryptocurrencies history

The history of cryptocurrencies is now almost ten years old. The first concept for the first cryptocurrency was created in 2008. This is the concept known as Bitcoin. The inventor is not known to the public until now. The only reference to the creator(s) is the pseudonym Satoshi Nakamoto under which the first paper on the matter was published in 2008 titled “Bitcoin: A Peer-to-Peer Electronic Cash System”.[8]

The history of cryptocurrencies is also the history of Bitcoin. Bitcoin was the first ever digital currency and is still the most best-known crypto coin worldwide. The first idea of a digital currency based on cryptography dates back to the end of the last millennium, specifically to the year 1998. At that time, Nick Szabo published his ideas on a purely digital currency and in that context spoke of the "bit gold".

After that, it took another ten years for Satoshi Nakamoto to develop the first concept for Bitcoin as a digital currency. The Bitcoin network itself started one year later, in 2009. In January that year, the first 50 Bitcoins were created by the so-called mining process. At that time no one expected what enormous value increases would be ahead.[9]

After the introduction of Bitcoin, it took two more years until with Litecoin another cryptocurrency was developed. Overall, there existed barely more than ten digital currencies until 2014, but the "hype" began slowly, starting in 2015. Among the historically earliest digital currencies with the respective year of publication belonged:

- Bitcoin: 2009
- Litecoin: 2011
- Bytecoin: 2012
- Ripple: 2013
- Dogecoin: 2013
- Dash: 2014
- Ethereum: 2015[10]

The history of Bitcoin is still representative for the history of cryptocurrencies as such. Therefore, a look at the history of digital currencies definitely includes a look at the price trend Bitcoin has had over the past decade. In the first year, in 2009, there was still no value relationship with a known central bank currency. For the first time in 2010, some market participants began to place the Bitcoin in relation to the US dollar. Between 2010 and 2013, one Bitcoin - except for short interim jumps – was rarely worth more than a dollar.[11]

However, there was a veritable price explosion in 2014, when Bitcoin first jumped over the mark of 1,000 Dollars. Nonetheless, the value dropped relatively quickly back to below 500 Dollar. One bitcoin had not yet passed the 1,000 Dollar mark in early January of the year 2017 but in late 2017 it was worth more than 20,000 Dollar for a short period of time, followed by a dramatic decrease in price.

[5] AndreasAntonopoulos, Mastering Bitcoin: Programming the open Blockchain (Sebastopol: O’Reilly Media, Inc, 2017), 9-11.

[6] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 80.

[7] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 5-6.

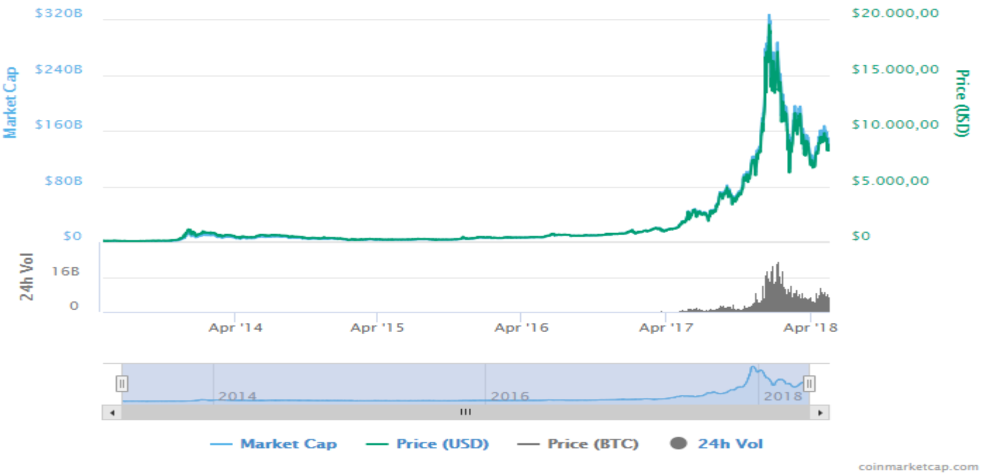
[8] SatoshiNakamoto,“Bitcoin: A Peer-to-Peer Electronic Cash System”, accessed May 19, 2018, https://bitcoin.org/bitcoin.pdf.

[9] Swan Melanie, Blockchain: Blueprint for a new economy (Sebastopol: O’Reilly Media, Inc., 2017), 3-4.

[10] “Cryptocurrency Overview”, Cryptocompare, accessed May 7, 2018, https://www.cryptocompare.com/coins.

[11] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 1.

Figure 1 – Bitcoin Price-Chart (USD)



(Source: coinmarketcap.com, Accessed May 5, 2018)

3. Bitcoin & Altcoins Technology

A. An Introduction to the Blockchain

While Bitcoin is by far the best-known and most successful example of blockchain-based technologies, the two terms are not synonymous.

The scope of blockchains goes far beyond crypto-currencies: "smart contracts," administrative bureaucracy, online voting, or, more broadly, a new form of the Internet - not just the financial sector may face a blockchain-induced upheaval.

At the beginning of each Blockchain is a network of users (nodes) that are interconnected (a peer-to-peer network) and in some way have transactions based on trust. These can be financial transactions, but also the conclusion of an insurance or the reallocation of a property or any other information.[12]

Usually, for such a business, a middleman is installed, a so-called "trusted third party". In the case of a money transfer, this would be, for example, the banks where the paying party and the recipient have their accounts. For other payment transactions, other service providers, such as credit card providers, are interposed. All these middlemen slow down the process of the transaction; they also charge fees for their services, making the transaction even more expensive.

With a blockchain, there is no need for a "trusted third party", which is why we speak of a "trustless system".[13]To understand a Blockchain, it is necessary to understand the technical and mathematical foundations. At the beginning of each Blockchain there is a record, which, as mentioned above, can be different things, for the sake of clarity, we assume a financial transaction in this example.[14]

For each transaction a hash value is being calculated. In the case of financial transactions, the data of the transaction is assigned a string with a defined length by a hash function. This can be a larger amount of data, summarized by a smaller one - the hash value. Since this is a mathematical function, it always remains comprehensible which record hides behind the hash value. Because of this property, the hash value is also referred to as a "fingerprint of digital data". Several of these transactions are combined into one block. Each block can be identified by a specific string. This string, the so-called "block header", also contains a hash value. This hash value results from the summary of the hash values of all transactions of the block. These blocks are then linearly concatenated. In addition to the information about the transactions of the block, the block header also contains the hash value of the preceding block.[15]

In this system, individual transactions cannot be changed without changing the entire chain. This is because changing the transaction data also changes their hash value and thus also the hash value in the block header of the respective block and subsequently also all subsequent blocks. Each new transaction carries the sum of all previous transactions.

[12] Swan Melanie, Blockchain: Blueprint for a new economy (Sebastopol: O'Reilly Media, Inc., 2017), 94.

[13]Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 140-3.

[14] Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 27-30.

[15]Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 106.

It is therefore not necessary to involve a third party to ensure whether the counterparty actually has the financial means to pay a certain amount. Since all previous transactions are available on the Blockchain, it can easily be verified at any time how much money each participant of the network possesses.

For privacy reasons, all agentson the Blockchain appear under a pseudonym. Thus, the blockchain is fraud-proof because it is always possible to track all transactions while hiding the identity of the participants.

This system on its own would not be completely tamper-proof. An even more secure Blockchain must prevent new blocks from being created as desired. Therefore, creating new blocks on the blockchain is tied to a mathematical puzzle. Extensive testing requires finding a specific combination of characters that corresponds to a predetermined target value. This process is called mining. The difficulty of the puzzle is steadily adjusted by an algorithm to create new blocks at regular intervals.[16]

Solving this puzzle takes time and computing power. The one who delivers the right solution first gets a reward. What exactly this reward looks like differs from Blockchain to Blockchain, on the bitcoinBlockchain miners are rewarded with newly created bitcoins. A further result of mining is, that it validates the transactions in the newly created block. Since mining is very costly and time-consuming, larger blockchains will not allow ordinary users to participate in it – without economical disadvantages - bitcoin mining is taking over commercial data centers with specialized hardware.[17] In the original Blockchain concept by Satoshi Nakamoto, Miner, Nodes and User were identical. To use Bitcoin, a node had to be set up first. To do this, you had to download and save the entire blockchain with all the transactions and then participate in verifying transactions and blocks, meaning each node could (and should) act as a miner.[18]

However, with the specialization and commercialization of mining, the roles soon separated. Specialized hardware and ever-increasing technical requirements meant that mining could only be reasonably and profitably operated by data centers.[19]

At the same time, better and better wallets have been published, enabling trading on the Bitcoin Blockchain without even participating in the network. Wallets are applications that serve only to initiate transactions on the blockchain. A single server assumes the role of a node, through which various users can communicate with the network without having to store the blockchain itself.[20]

Only the nodes ensure that the blockchain is replicated. They ensure that the blockchain remains tamper-proof by downloading and saving the blockchain and reviewing and distributing the ever-growing stream of transactions.

3.1. What is a Hash?

Hash value is a term used in computer technology in the field of cryptology and denotes an alphanumeric value that is generated by a special form of the hash function. The peculiarity of this mathematical function is, that it maps an arbitrarily long string to a string of fixed length. In practice, the hash value is often a string of 32 or 64 characters. The hash has a one-way character.[21]This means that although the same hash value always arises from a certain string of data with defined character length, conversely, from this figure it is not possible to recalculate the original value. These properties make hash values attractive for a variety of applications, such as the following:

- Storage of passwords: Instead of the password itself, in computer applications with required login, the hash value of a password is often stored instead of the password itself for the authentication. If the password is entered when logging on to the system, the hash value is generated from this and compared with the already stored hash value.
- Data integrity: Since hash functions applied to identical data always provide the same values, it can be checked in this way whether data has been distorted during transmission over an insecure network.[22]

An example for hash algorithm is SHA-256 used within the Bitcoin network.

[16] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 49.

[17]Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 76.

[18]SatoshiNakamoto,"Bitcoin: A Peer-to-Peer Electronic Cash System", accessed May 19, 2018, https://bitcoin.org/bitcoin.pdf.

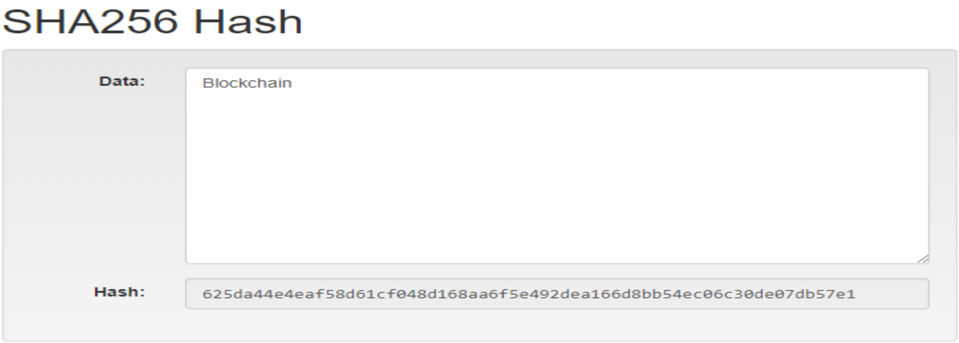
[19] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 33.

[20]Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 5-9.

[21] Akashi Staoh, "Unified Hardware Architecture for the Secure Hash Standard," in Embedded Cryptographic Hardware: Methodologies and achitectures, ed.Nedjahand de Macedo (New York: Nova Science Publishers, Inc, 2004), 1-16.

[22]Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 82-5.

Figure 2 – Sha256 Hash Value of A Data string



SHA256 Hash

Data: Blockchain

Hash: 625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1

(Source: Own Research)

The figure above shows the hash value of the data input “Blockchain” as an output of the SHA256 hash algorithm.

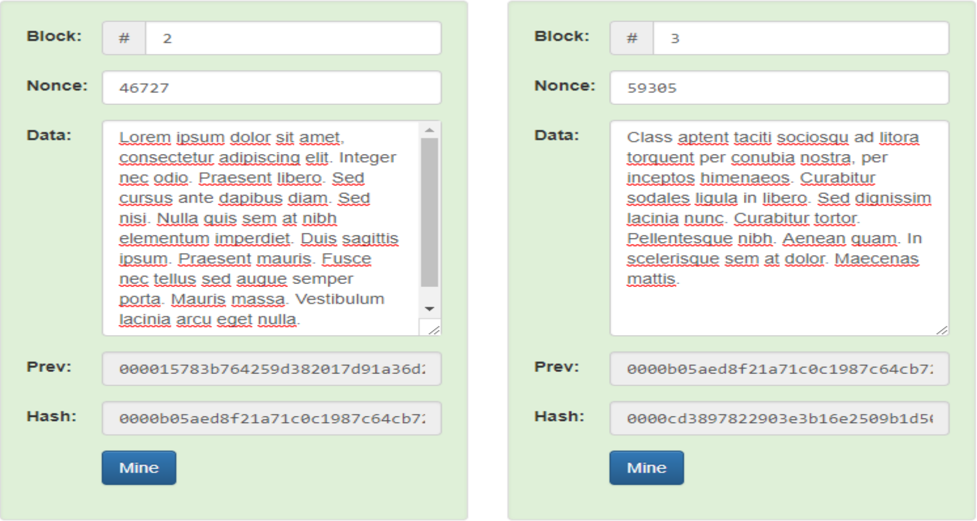
3.2. What is a Block?

Basically, blocks exhibit a very simple structure. There is an area with metadata, the header, as well as an area for the payload,the individual transactions that are combined in one block. The average number of transactions fluctuates greatly, with between about 1,300 and 2,100 transfers per block over the past year on the Bitcoin Blockchain.[23]

The header of a block contains a dozen of fields that are only partially self-explanatory. On the one hand there is pure informational data, on the other hand the hashes. The block information includes data such as creation date, size or number of transactions. The hashes ensure the integrity of the database. Since the hash of the current block has processed the data from the previous block, the integrity of the blockchain is ensured - one could not change a block hash without also changing the block before and of course subsequent blocks.[24]

There is one thing special about the hashes within the Bitcoin Blockchain, since they all start with "00000000000000000". This is the result of the proof-of-work consensus algorithm, the cryptographic puzzle that must be solved to create a new block. The goal is to find a hash to a block that just begins with this series of zeroes. This works changing the so-called Nonce as long as the whole data string gets a specific value without changing the transactional data.[25]

Figure 3 – Sha256 Hash Value of a Data string



Block: # 2

Nonce: 46727

Data: Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer nec odio. Praesent libero. Sed cursus ante dapibus diam. Sed nisi. Nulla quis sem at nibh elementum imperdiet. Duis sagittis ipsum. Praesent mauris. Fusce nec tellus sed augue semper porta. Mauris massa. Vestibulum lacinia arcu eget nulla.

Prev: 000015783b764259d382017d91a36d

Hash: 0000b05aed8f21a71c0c1987c64cb7

Block: # 3

Nonce: 59305

Data: Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur sodales ligula in libero. Sed dignissim lacinia nunc. Curabitur tortor. Pellentesque nibh. Aenean quam. In scelerisque sem at dolor. Maecenas mattis.

Prev: 0000b05aed8f21a71c0c1987c64cb7

Hash: 0000cd3897822903e3b16e2509b1d5

(Source: Own Research)

[23] Meinel and Gayvoronskaya and Schnjakin, Blockchain: Hype oder Innovation (Potsdam: Universitätsverlag Potsdam, 2018), 36-40.

[24] Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 71-2.

[25] Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 90.

Figure 2 shows the schematic structure of a block. The figure shows the most important values such as the number of blocks, the nonce, the data, the hash value of the previous block and the new hash value of the current block. The picture shows, that block “3” is containing the previous hash value information to become a chain of blocks.

In addition to the hashes, a "Merkle Root" is also specified. This hash tree root is used to cryptographically secure the transactions in the block and their correct order. So not only blocks cannot be changed, also the transactions within the blocks are safe.[26]

The header contains all sorts of metadata that is relevant for analysis and understanding. Particularly important from a management point of view are the number of transactions, the transfer volume, the transaction fees and the so-called block reward, the reward the miner gets for the creation of the block, so ultimately finding the hash with the leading zeros. Actually, the block reward is 12.5 BTC (Bitcoin) per block. Every 210,000 blocks the reward is halved.[27]For understanding the cryptographic puzzle there are at two important values: difficulty and nonce. The difficulty (of the cryptographic puzzle) is a value that ensures blocks emerge every 10 minutes. In addition, in the case of competing blocks, the one with the higher difficulty is preferred.[28]

Of course, a block has a specific hash by default, which usually does not start with a bunch of zeros. To achieve a hashing with leading zeros, an additional date is appended to the hash block - until the hash is just “0000000000000000XYZ”.

The other values in the header are basically: timestamp, receive time, bits, size and version of the block header.[29]
Behind the header there is the actual information data. Transactions consist of one or more sending and receiving accounts, represented as hashes, the IDs of the users or wallets. In a Blockchain explorer, all of these accounts and transactions are clickable links, so it's easy to see in the browser who sent what and when.

Noticeable is the first transaction of each block. Here is usually a message such as "No inputs (newly generated coins)". This so-called Coinbase transaction is the transfer of the block rewards for the miner - so there are no existing coins transferred, but new coins generated.

Internally, transactions also have all sorts of data fields such as size, date, block number or number of incoming and outgoing accounts as well as hashes of themselves and the preceding or following transaction.[30]

3.3. Smart Contracts

A Smart contract, besides being a platform for currencies, is one of the most promising applications of a Blockchain. In smart contracts, a contractual rule is written down as code that follows a conditional logic, it follows an "if-then" pattern: if certain conditions are met, a specific contract term automatically comes into force. While third parties, such as attorneys, usually guarantee that a contract is being honored, smart contract technology ensures compliance with the contract - so there is no need to interpose an intermediary institution to ensure trust between contractors.[31]

Supporters of smart contracts are hoping the technology will ease business processes and fulfillment, as well as enhancing contract security

The Blockchain Ethereum serves as a platform for crypto-currency ethers, while the Blockchain Smart Contracts can be used to create, manage and execute. In Ethereum, Smart Contracts exist as accounts that resemble those of users (user accounts), but are not controlled by a private key, but by the code contained within them.

Currently, the blockchain Ethereum has become the platform for smart contracts. This is primarily because the oldest and largest blockchain Bitcoin is not designed for the use of smart contracts in its protocol.

You can communicate with these smart contracts, just like any other account, but the contract itself cannot be changed once it's created and stored on the Blockchain. That makes it immune to hacker attacks from the outside. The contracts could then be traded like cryptocurrencies, but their content would not be a static monetary value, but a particular code that responds to "if-then" events as described above.[32]

[26] Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 92.
[27] Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 39.
[28] Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 105.
[29] Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 11.
[30] Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 122.
[31] Meinel and Gayvoronskaya and Schnjakin, Blockchain: Hype oder Innovation (Potsdam: Universitätsverlag Potsdam, 2018), 64-5.
[32] Sunith Shetty, ed., Ethereum Smart Contract Development (Birmingham: packt Publishing Ltd., 2018), 3-5.

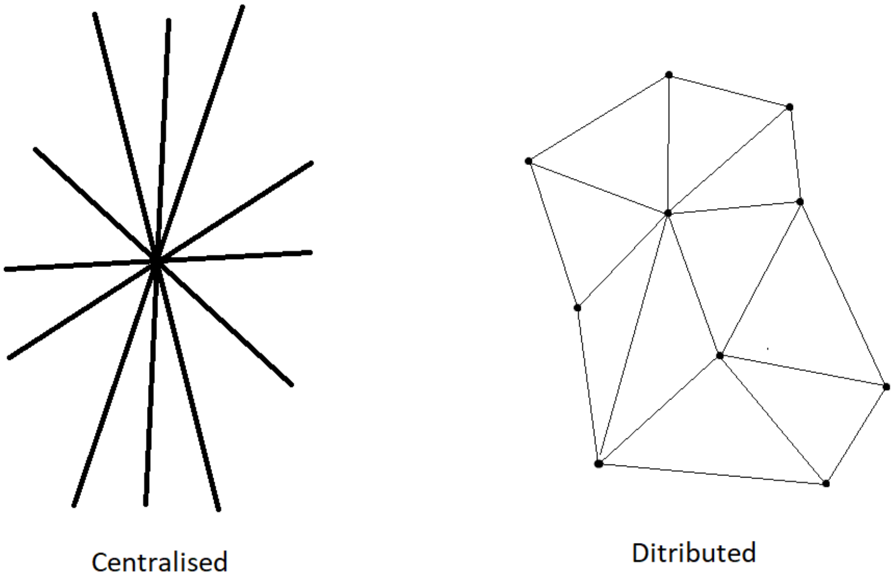
It is currently not clear which route the development of smart contract technology will take. However, there is a whole lot of possible applications. Dapps (distributed apps) can be created on the basis of various smart contracts that are linked to each other.[33]

Of course, any form of purchase or lease could be handled through a blockchain and even political elections could be held through blockchains. In theory, this is faster, cheaper, and more efficient, as bureaucratic administrative structures could be saved, and third parties that previously provided security for contractors (such as lawyers, banks, or insurance companies) would become redundant. In practice, however, we are still a long way from that.[34]

3.4. Centralized vs. Decentralized vs. Distributed

In a decentralized or distributed structure, there is no institution or center that controls and monitors the monetary system. This happens with decentralized networks like Bitcoin by the members themselves (P2P).[35]

Figure 4 – Zentralized Vs. Dezentralised Design



(Source: Own Research)

For decentralized cryptocurrencies there is no single point of failure. If one component of the system fails, it can still exist. This is usually not the case with banks. As we learned in 2008 and beyond, in the end, citizens had to pay for the system. Systemically, important banks were saved by the taxpayer – the motto: "too big to fail".[36]

Although most cryptocurrencies are decentralized, not all cryptic currencies are created decentrally. Some are centrally produced by owner-managed, private-sector companies, such as the Ripple.[37]

The Ripple (XRP) is created by the for-profit company Ripple Labs, which retains 80% of new issues and distributes them at its own discretion.[38]

3.5. Security, Cryptography and Anonymity

All Bitcoin transactions are publicly and permanently stored on the network, which means that anyone can see the balance and transactions of each Bitcoin address. However, the owner's identity cannot be associated with the Bitcoin address until the owner reveals information as part of a transaction or otherwise.[39]

[33] Sunith Shetty, ed., Ethereum Smart Contract Development (Birmingham: packt Publishing Ltd., 2018), 39.

[34] Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 27-30.

[35] Meinel and Gayvoronskaya and Schnjakin, Blockchain: Hype oder Innovation (Potsdam: Universitätsverlag Potsdam, 2018), 221-3.

[36] Swan Melanie, Blockchain: Blueprint for a new economy (Sebastopol: O'Reilly Media, Inc., 2017), 5.

[37] Meinel and Gayvoronskaya and Schnjakin, Blockchain: Hype oder Innovation (Potsdam: Universitätsverlag Potsdam, 2018), 74.

[38] Schwartz and Youngs and Britto, "The Ripple Protocol Consensus Algorithm", accessed May 2, 2018, https://ripple.com/files/ripple_consensus_whitepaper.pdf

Cryptography is at the heart of Bitcoin. The only problem is that modern cryptography is hard to understand. The simplest definition of encryption is that it should protect information from third parties. It has been like that for a long time and always will be. Whether in war, in diplomacy or on the Internet. If you want to entrust a person with a secret, it is best to meet privately with this person in a safe room. For obvious reasons, this is not always possible.

Even the ancient Romans knew this problem. How does the emperor tell his troops in Germania that they should withdraw? If one writes this command on a parchment and lets a rider carry this over, one runs the risk that the rider is overwhelmed by the enemy and the message is used against the Roman troops.

The Romans have therefore used a simple encryption, which is named after the great commander of the Caesar code: Each letter in the alphabet is replaced by another letter. ABCDEFGHIJKLMNOPQRSTUVWXYZ becomes FGHIJKLMNOPQRSTUVWXYZABCDE. Each letter is shifted 5 letters to the right. The number 5 in this system is the secret key known to both the emperor and the commanders. However, in modern days this is not an efficient way of encrypting data.[40]

Cryptography is mathematics. Asymmetrical encryption works by encrypting with one key and decrypting with the other. Blockchains are based on an asymmetric cryptographic method that differentiates between public and private key.

When sending the digital fingerprint of a data string, the data has to be protected from getting manipulated.

Each member of the blockchain has a private and a matching public key. A private key creates a unique digital signature of the data. The hash of the data is encrypted with an associated public key. The resulting string is equated with a signature. The recipient of the digital fingerprint will also be sent the public key within the transaction. This is a derivation of the private key and makes it possible to verify the created signature. Consequently, the receiver gets the hash of data.[41]

The recipient of the public key can also verify in this way that only the sender could have signed this hash. Only the published public key of the sender can decrypt the encrypted hash. Thus, ownership rights in the blockchain are clearly disclosed.[42]

However, it is impossible to guess through the public key what the matching private key looks like. Namely, the creation of a public key is based on a similar method as the generation of the character string by the block signing hash algorithm. Whoever is in control of the private key, controls the assets it is linked to.[43]

3.6. Attack points of a blockchain

Blockchain systems are based on proven encryption systems, which basically prevent many attacks. For example, attackers are unable to generate transactions from accounts whose credentials they do not own. Outgoing transactions must be cryptographically signed with these access data.

However, relevant blockchain systems are complex and geographically dispersed, theoretically allowing some kind of attacks. Regardless of their technical vulnerability, blockchain deployments are often largely unregulated and prone to fraudulent trades.

If an attacker controls the Bitcoin network, for example by taking over more than 50 percent of the computing power of the network, a fraudulent attack is possible. The attacker can isolate his part of the network, send a transaction to the smaller remainder of the network, and have it validated. However, the attacker's network may continue on an alternative blockchain without the transaction and transmit it to the smaller part of the network at any time. Since the alternative blockchain involves more computational power, it overwrites the blockchain that contains the transaction - it has been confirmed, done, but in retrospect it did not happen.[44]

[39] Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 111-3.

[40] R. F. Churchhouse, Codes and ciphers: Julius Ceasar, the Enigma, and the Internet (Cambridge: Cambridge University Press. 2002), 1-3.

[41] Meinel and Gayvoronskaya and Schnjakin, Blockchain: Hype oder Innovation (Potsdam: Universitätsverlag Potsdam, 2018), 21-2.

[42] Daniel Drescher, Blockchain Basics: A non-technical introduction in 25 Steps (Frankfurt am Main: Springer Verlag, 2017), 100.

[43] Narayanan et al., Bitcoin 12.5: A Compehensive Introduction (New Jersey: Princeton University Press, 2016), 80-82.

[44] Meinel and Gayvoronskaya and Schnjakin, Blockchain: Hype oder Innovation (Potsdam: Universitätsverlag Potsdam, 2018), 49-51.

In practice, no hack of a blockchain is known yet. However, many people lost their funds by careless handling of their private key. Attackers can also take control of computers by phishing or exploiting vulnerabilities. Then it is easy for the attacker to read access data stored on the computer. A remedy is to set passwords for access to access data or to use a hardware wallet that signs the transactions without the access data ever being stored in the memory of the computer being used.[45]

There have also been attacks on crypto-exchanges. Around 850,000 Bitcoin attackers were able to take over in 2014 by hacking the Bitcoin exchange Mt. Gox. Bitcoin exchanges need to store the credentials themselves to manage the accounts for their clients - and may therefore lose them. The hack of Mt. Gox is not the only known hack of an exchange.[46]

4. Obtaining Cryptocurrencies

4.1.Crypto-Exchanges

Cryptocurrencies can be bought online on so-called exchanges. Enthusiasts and digital currency investors are meeting there to purchase and trade cryptocurrencies. Bitcoin, Ethereum and other currencies are directly interacting with each other, so that the price is formed by supply and demand,

On these exchanges, registered users may submit offers to buy or sell Bitcoins with a different currency. A deal is made as soon as an offer is accepted by the buyer and the seller. Depending on the marketplace, the operators charge a small fee for the successful brokerage of the trade. Buyers and sellers usually pay half of each of these fees.

Trading on the crypto exchanges is automated. The trades on a marketplace, however, are handled manually, so you have to search for a suitable offer yourself. The conventional currencies US dollar or euro can be exchanged on the crypto exchanges against Bitcoins or other Internet currencies.[47]

Table1 – Top 10 Cryptoexchanges (Volume USD)

Rank	Exchange Name	Markets	24h Trades	24h Volume	Marketshare
1	Bitfinex	143	>314,511	$1,506,074,538	33%
2	Binance	224	>3,256,420	$1,194,297,329	26%
3	HitBTC	311	>423,266	$257,487,868	6%
4	Coinbase GDAX	12	>162,281	$254,193,290	6%
5	Quoine	26	>110,218	$226,196,403	5%
6	Bithumb	12	>183,876	$157,016,102	3%
7	Bitstamp	11	>68,236	$141,723,539	3%
8	coinone	6	>168,901	$125,349,982	3%
9	EXX	30	>54,354	$84,408,697	2%
10	BTC-e / WEX	26	>40,980	$82,357,298	2%

(Source: https://cryptocoincharts.info/markets/info, accessed May 19, 2018)

Table 1 shows the top 10 biggest crypto-exchanges ranked by trading volume in USD per day. Actually, there are 200 existing crypto exchanges with a total day volume of 4,80 billion USD.

4.2. Mining

Miners act as auditors on currencies such as Bitcoin and Ethereum. They confirm the correctness of the transactions, as a kind of witness that person A has sent person B a certain amount of Bitcoin. One block on the Bitcoin Blockchain contains one megabyte of data. Depending on how much information the transactions contains, one megabyte could theoretically be just one transaction but mostly there are several hundreds. There is also a reward for verification of the transactions contained in the mined block. Depending on the transaction volume, this is currently between 0.4 and 2 Bitcoin. Additionally, they get 12.5 bitcoin to create a block.[48]

[45] Swan Melanie, Blockchain: Blueprint for a new economy (Sebastopol: O'Reilly Media, Inc., 2017), 82-3.

[46] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 163-8.

[47] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 71.

[48] Elfriede Sixt, Bitcoin und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie (Wiesbaden: Springer Gabler, 2017), 101.

The reward for creating the block is to ensure that as many people as possible are mining. That's an extra safety measure. For if a miner should verify a block that is flawed, indicating a manipulation, all miners will vote on whether the block is accepted. The more computational power a miner spends on building blocks, the greater his voting poweris within the network.[49]

Because it takes a lot of computational power to create a block, it is highly unlikely that a single miner will have 51 percent of the total computing power in the Bitcoin network. If a miner had that much power, a so-called 51-percent attack would be possible.[50]

The high rewards of 12.5 Bitcoin, equivalent to $ 125,000 at $ 10,000, attract many miners. Many different miners mean a decentralized distribution of computing power. This makes it harder for a single miner to reach 51 percent.

12,5 BTC as a reward may look strange at first sight. The amount of the reward is halved every 210,000 blocks. In 2009 there were 50 Bitcoin as a reward, in November 2012, the cut came to 25. Since mid-2016, there are 12.5.[51]The next halving is expected in mid-2020. At bitcoinclock.com there is a countdown until the next cut.[52]

As the reward system adds only incremental units of the cryptocurrency, strong inflation is prevented. Theoretically, it should also work in the opposite direction: With the increasing interest in Bitcoin, there are more users and thus more demand. More offered coins should satisfy the demand and counteract a dramatic price increase. This has not worked out due to the Bitcoin hype: In early 2017, the price was under $ 1,000, in December 2017, the $ 20,000 mark was cracked.

In addition to halving, there is also a limit on the maximum amount of eligible coins. There will be 21 million bitcoins, after which there will be no more rewards for building blocks. This is expected to happen in 2140. Presumably in the year 2032 99 percent of all Bitcoin will be in circulation. At this time, the reward will have fallen to less than one bitcoin per block.[53]

With more Bitcoin in circulation, the transaction volume is expected to be higher. As a result, miners are collecting more bitcoin from the transaction fees and will continue to mine, keeping the blockchain alive.

The actual task, verifying the transactions in size of a MB, takes only 0.2 to 0.4 seconds and can be done with a regular computer. Why is so much talk about the high computational effort and power consumption in mining? To maintain the decentralized structure of Bitcoin and prevent the 51 percent attack from occurring, the miners compete against each other to receive the reward. Although this competition is often referred to as "solving mathematical puzzles", it is actually a guessing game. This concept is called "proof of work".[54]

The first miner to guess the given hexadecimal number, called Target Hash, or a value below, is the winner. If there is a tie, the Bitcoin network decides by a majority vote. Usually, the miner that has invested the most computing powergets the price. Miners need to guess a number-of-only-used nonce, which is 32-bit in Bitcoin. The nonce is added to the known values of the creating block. The whole thing is then hashed again. If the result matches the target hash the block is signed.[55]

The chance to guess the right nonce is influenced by the level of difficulty. This level of difficulty depends on the total computing power in the Bitcoin network and is adjusted every 2,016 blocks. If there are fewer miners and the computing power drops, the difficulty level drops. If there are more miners, it will rise.

The difficulty level varies to maintain an average time of ten minutes per new block. The ten-minute interval was set by Bitcoin inventor Satoshi Nakamoto. When creating the concept for bitcoin, he thought that it takes a minute for all miners to know that a new block has been created and can therefore proceed with the creation of the next block. The one minute in which they unnecessarily dig for a block that already exists, at the ten-minute interval is a waste of 10 percent of the computing power of the network.[56]

[49] Jose Pagliery, Bitcoin: And the Future of Money (Chicago: Triumph Books LLC, 2014), 44.

[50] Elfriede Sixt, Bitcoin und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie (Wiesbaden: Springer Gabler, 2017), 106.

[51] Antony J. Malone, Glossary of Bitcoin terms and definitions (Toluca Lake: NoHoMedia, 2015), 3.

[52] Albert Szmigielski, Bitcoin Essentials (Birmingham: Packt Publishing Ltd., 2016), 25-9.

[53] Antony J. Malone, Glossary of Bitcoin terms and definitions (Toluca Lake: NoHoMedia, 2015), 1.

[54] Albert Szmigielski, Bitcoin Essentials (Birmingham: Packt Publishing Ltd., 2016), 85.

[55] Albert Szmigielski, Bitcoin Essentials (Birmingham: Packt Publishing Ltd., 2016), 15.

[56] Elfriede Sixt, Bitcoin und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie (Wiesbaden: Springer Gabler, 2017), 41.

VI. References

Antonopoulos, Andreas. Mastering Bitcoin: Programming the open Blockchain. Sebastopol: O'Reilly Media, Inc, 2017.

Churchhouse, R. F. Codes and ciphers: Julius Ceasar, the Enigma, and the Internet. Cambridge: Cambridge University Press, 2002.

Cryptocompare. "Cryptocurrency Overview." Accessed May 7, 2018. https://www.cryptocompare.com/coins.

Cryptocoincharts. "Exchange, Volume." Accessed May 19, 2018. https://cryptocoincharts.info/markets/info.

Drescher, Daniel. Blockchain Basics: A non-technical introduction in 25 Steps. Frankfurt am Main: Springer Verlag, 2017.

Meinel, Christoph,and TatianaGayvoronskaya,and Maxim Schnjakin. Blockchain: Hype oder Innovation. Potsdam: Universitätsverlag Potsdam, 2018.

Malone, J. Antony. Glossary of Bitcoin terms and definitions. Toluca Lake: NoHoMedia, 2015.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System", Accessed May 19, 2018. https://bitcoin.org/bitcoin.pdf.

Narayanan, Arvind, and Joseph Bonneau, and Edward Felten, and Adrew Miller, and Steven Goldfeder.Bitcoin 12.5: A Compehensive Introduction. New Jersey: Princeton University Press, 2016.

Nedjah, Nadia, and de Macedo Mourelle, Luiza, 1-16. New York: Nova Science Publishers, Inc, 2004.

Pagliery, Jose. Bitcoin: And the Future of Money. Chicago: Triumph Books LLC, 2014.

Schwartz, David, Noah Youngs, Arthur Britto. „The Ripple Protocol Consensus Algorithm", Accessed May 2, 2018. https://ripple.com/files/ripple_consensus_whitepaper.pdf

Shetty, Sunith, ed. Ethereum Smart Contract Development. Birmingham: packt Publishing Ltd, 2018.

Sixt, Elfriede. Bitcoin und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie. Wiesbaden: Springer Gabler, 2017.

Staoh, Akashi. "Unified Hardware Architecture for the Secure Hash Standard." In Embedded Cryptographic Hardware: Methodologies and achitectures, edited by

Swan, Melanie. Blockchain: Blueprint for a new economy. Sebastopol: O'Reilly Media, Inc, 2017.

Szmigielski, Albert. Bitcoin Essentials. Birmingham: Packt Publishing Ltd, 2016.