PROJ 201 Project Final Report

Project Title:A Survey on Cryptocurrency

Name, Surname & ID of group members:Fatih Arda Zengin 28031, Gazi Furkan Bakar 26502, İsmail Berat Düzenli 28037

Supervised by:Kamer Kaya

Month, day, year: 01/03/2021

Abstract

The Internet provides lots of opportunities to people since it has spread over the world. Digital currencies were one of them to give privacy to people in expenses in contrast to government and bank-controlled money. The most popular one Bitcoin firstly announced in 2008 and opened public in 2009 promising a non-centralized, no permission required, blockchain based digital currency. It was the correct time for society to rebel against authority-based money understanding and to declare freedom to that when corporations and governments lost reliance on society. After Satoshi Nakamoto launched Bitcoin, it was followed by other developers. They created different types of currencies that have different purposes, technical layers, utilities, legal status or underlying values in years. But all of these became popular with an unprecedented rise in the values of these currencies in 2017. People started to ask, "What are they?"," How can I buy?", "Are they legal?", "Are they reliable?"," How can I know its value will increase?". In this project, we are going to find answers to these questions, create basic criteria to explain features of cryptocurrencies, evaluate some of the classic coins by looking at whitepapers, social media accounts of developers, CVs and network of developers, user experiments, websites of these coins. In addition to that, we will point out the privacy of these coins and are they as private as most people think. Then we are going to look at privacy-oriented coins from a similar perspective to see are they provide what they promise.

Introduction

The economic crisis, which started in the United States in 2007 and affected the whole world economic system in early 2008 emerged because of debt which belongs to households all around the world especially in the United States. This economic crisis deepened by the bankruptcy of Lehman Brothers which is the fourth largest investment bank in the United States of America. The Federal Reserve tried to save the banks with 700 billion dollars rescue pack. Meanwhile, most of the other global economies announced similar recovery packs that were funded by citizen's taxes.

Two of the issues which are relevant to banks and governments destroyed the public trust in the central authorities. This situation made the public feel the need for alternatives. All of these led to the creation of Bitcoin and the tech behind it which is blockchain. In October 2008 an anonymous user who is using Satoshi Nakamoto nickname published an article named "Bitcoin: Peer-to-Peer Electronic Cash System" on a website called metzdowd.com which is mostly used by cryptology fans. This article includes how Bitcoin and Blockchain can work decentralized and without any intermediary. In January 2009 first block of the system was released and it includes a text which is a reference to the 2008 financial crisis. It was a Times title dated 3 January 2009 which is "chancellor on brink of second bailout for banks".

Purpose

Cryptocurrencies get attention since the extreme rise of their, especially bitcoin, price in 2017. This was a good opportunity to present themselves to the world. On the other hand, these unprecedented rises in prices caused the attention of lots of uninformed people who want to just make money without research. This led to an increase in the number of cryptocurrencies that are not good intended or poorly qualified cryptocurrencies. On the other hand, we think this technology is going to become a more serious and common tool in our daily life. As a result of that, we want to clarify concepts of cryptocurrencies and explain what are these commodities, what is standing behind them, how reliable they are, when they should be bought or sold, which ones should be bought or sold. We will try to define key points to indicate a cryptocurrency is whether valuable or not. We will make criteria which include different aspects of cryptocurrencies like centralization, privacy, the security of the network, speed, market cap, volume, etc. and range of value which can be delivered by a cryptocurrency according to its features and its purpose and a final outcome to determine how proper this currency is to give an idea to investors or corporations thinking to establish a partnership with these projects. We will cover classical coins such as BTC (Bitcoin), ETH (Ether, Ethereum), BCH (Bitcoin Cash), BSV (Bitcoin SV), LTC (Litecoin), XRP (Ripple), BNB (Binance Coin) to give an idea about most used and invested coins. In addition to that, since some investors can want to be hidden while making transactions, we will focus on privacy tokens because lots of people think Bitcoin and other altcoins are completely private and untraceable, but they are not. However there are some altcoins give their users this, such as XMR (Monero), ZEC (Zcash), DASH which promise their user to be hidden while making a transaction in terms of the amount of transaction and sender and taker addresses. Eventually, we are going to prepare a report to investors who want to invest in cryptocurrencies about a guideline and advise how to invest and invest in what.

Description of Specific Steps

We examined studies on e-cash. Put these in chronological order. We elaborated on blockchain technology to better understand cryptocurrencies. We read the white papers of the main cryptocurrencies such as Bitcoin, Ethereum, Bitcoin Cash, Bitcoin SV, Litecoin, Ripple, Binance Coin. We also read the white papers of cryptos such as Monero, Zcash, DASH, which are called privacy tokens. We sew if it is decentralized and then tried to rate its reliability if it has a center. Cryptocurrency's market value, speed, network security, privacy, market volume, and volatility is

judged. We examined studies of cryptocurrencies such as Ethereum 2.0. This varied depending on the scoring advantage or disadvantage. In addition, the current price of cryptocurrencies and the past price was evaluated. We gathered these statistics from coinmarketcap.com. As a result of this scoring, each cryptocurrency had a comprehensive evaluation.

Glossary

Address: It is an alphanumerical code that is used to send and receive cryptocurrency on blockchain
Altcoin: Alternative coins of Bitcoin
ASIC (Application-specific integrated circuit): Complicated hardware which is specialized on mining.
ATH (All time high): The highest recorded price of a coin.
Bear, Bearish: The price that is prone to decrease.
Block: Data packages which is permanently recorded by blockchain network.
Blockchain: A kind of algorithm that record data in a decentralized way.
Bullish, Bull: The price that is prone to increase.
Double Spending: It is a kind of problem that allows to spend an amount of cryptocurrency two times.
Fork: It is a case when a change occurred on the source code, miners of the blockchain start to use different source code while mining.
Genesis Block: First block of a blockchain.
Hash: A cryptographic method to create a new value which differ from first value.
ICO (Initial Coin Offering): It is a way to crowdfunding that a startup launch its own cryptocurrency to raise funds.
Miner: People or programs which produce coin.
Mining: It is process of creating new cryptocurrency.
Node: A part of blockchain network.
Pool: Combining processing power of miners to mine together.
Satoshi: 1/100000000 of Bitcoin (0.00000001 BTC)
Token: It represent a specific commodity in a specific platform to use for specific purpose.
Volatility: Fluctuation in prices.

Results

Classic Coins

Bitcoin

Bitcoin is first cryptocurrency that depending on blockchain technology. It was generated by Satoshi Nakatomo who is still anonymous. Although there are people claiming themselves as Satoshi Nakatomo, nobody have proven it yet. Bitcoin's white paper is announced in 2008 that explaining weak sides of centralized financial institutions in terms of transaction cost and making small transactions harder and ability to reverse which allow fraud (Nakatomo, 2008) (coinmarketcap, n.d.). As a result of this weaknesses bitcoin aims to provide peer-to-peer so without central authority, not trust based, not third party needed, non-reversible financial system. (Nakatomo, 2008)

In 2009, Bitcoin Blockchain firstly launched. (coinmarketcap, n.d.). Technologies and concepts which were used in blockchain of bitcoin were not completely new things, it was synthesis of different concepts that released in different times and by different people since 1957 as referenced by Nakatomo (2008) in Bitcoin's whitepaper. First problem of a digital currency faced was double spending, while in a mint system central authority check every transaction. Bitcoin solves this problem by announcing every single transaction to public and providing same history agreement on the system participants. Firstly, Satoshi Nakatomo's (2008) solving way start with Timestamp Server Algorithm which is a system that create a chain that every block consists of limited amount of transaction and gives a timestamp as output by taking hash of block and previous block's timestamp. As a result of this algorithm, every transaction in chain is recorded and immutable because when a new block is appended to chain, it is impossible to change any previous block. But all of this process should be agreed by network and Satoshi Nakatomo's (2008) solution's second step is providing this agreement by Proof of Work. Proof of Work is an algorithm which is also used by other cryptocurrencies to ensure a consensus in blockchain network. It is working way is shortly that everyone has represented by its CPU power and when more than %50 of the network is agreed on same history rest of the system must accept majority's history. Long explanation of Proof of Work is hashes, which were mentioned while discussing Timestamp and are created by using block's transaction and previous block's timestamp are not directly created, in fact they are tried and found by "miners". There are lots of nodes and miners connecting each other to sustain blockchain environment, nodes have history of bitcoin transactions and they manage environment by approving blocks, and miners simply mine blocks (Binance Academy, n.d.). When transactions are made, these miners compete against each other to "mine" new block by bringing transactions together hashing the block with previous block. In this process, miners try to find correct hash value which gives required zero bits by trying which last average 10 minutes. When a miner found a solution in other words a suited value fitting the algorithm, it broadcasts this value and other nodes apply it to check (finding correct value by hashing is a determined process, it last average 10 minutes, even if

computing power of system increases, network sets its difficulty to ensure 10 minutes per block, but checking hashed value is simple and this leads to quick approval of new block). During approval process, there might be several created blocks by different miners. At this moment, nodes take first reached solution while keeping other options for other possible situations and miners start to work on new block. “Other possibilities” is that network goes through longest chain so if a new block came in addition to “reserved” block, then, node accept “reserve” block as correct and its addition block as new chain. In addition to that, Block that approved by most CPU power is recognized as accepted by rest of the network and chain continues through this block. As a result of this protocol bitcoin network become decentralized by distributing system running process to miners and nodes, avoid double spending by taking approval of lots of nodes and blocking altering or reversing spends by hashing new block by using previous blocks timestamp (Nakatomo, 2008).

As summarized by Nakatomo (2008) in Bitcoin’s whitepaper network has 6 steps to run:

1- Transactions become visible to all nodes

2- Nodes bring transactions together

3- Nodes try to find solution to hash function

4- If a node finds a solution, announces it to network

5- Nodes check block whether block is valid or not, also check that is there any double spending.

6- Nodes which approve new block start to “mine” a new block by using this blocks hash

So, all this system is run by nodes and miners, why they do this and why bad people cannot exploit proof of work algorithm by having majority of the power? Nodes are volunteers in reality but for miners answer is very well known today: Mining gives BTC reward from system and transaction fee from users to miners who mine a new block and make it approved by network. People become nodes to gain BTC so money and increasing number of people means increasing CPU power which makes capturing and exploiting network harder and too expensive. This reward system is also systematized by “halving”. (Binance Academy, n.d.)

Halving is an event that decreases bitcoin reward to its half when 210.000 new blocks created. At the beginning of the system reward for a block was 50 BTC, at 2012 halving it decreased to 25 BTC, at 2016 halving it decreased to 12.5 BTC, and at 2020 it decreased to 6.25 BTC which is current reward. Some people claim halving affect bitcoin by increasing its prices and they give evident as 2012 and 2016 halving events which increased bitcoin prices significantly: after 2012 halving event price went to 1.100$ from 11$ and after 2016 halving event bitcoin rose from 600$ to 20.000$ (Binance, 2020). In 2020 halving event which happened at may (Binance Academy, n.d.), bitcoin price rose from 9000$ to 23.000$ but it’s hard to estimate halving event’s role

especially in 2020 because of world's situation that includes Corona Virus, printing money and US elections. Even though impact of halving is controversial, it should be noted. If some people think halving event increases prices, it probably affects because of this perception. (coinmarketcap, n.d.)

Today, bitcoin is not same as how it founded in 2008. It is open source and licensed software by MIT and there are more than 750 developers developing bitcoin under the name of Bitcoin Core. Currently (December 2020) 241 patch have already announced and latest patch of Bitcoin Core is 0.20.1. (GitHub, n.d.). These patches come to existence by consensus of majority of network and developers but sometimes majority do not have consensus and some developers create a fork to bitcoin which uses bitcoin as base and make some differences. Bitcoin Blockchain has some important forks that offer different coins such as Bitcoin SV, Bitcoin XT, Bitcoin Classic, Bitcoin Cash, Bitcoin Gold (Reiff, 2019). It should be noted that Bitcoin Cash is important for this concept. Bitcoin cash and Bitcoin has lots of similar technical things like proof of work algorithm. But their philosophy is different in terms of size of one block due to some reasons including transaction speed and fee especially for microtransaction. Emergence of this Bitcoin Cash as a fork of bitcoins is a part of process called "civil war" by people due to these reasons (Frankenfield, 2020).

Bitcoin's price trend is upwards. Then, this trend and process power demanding proof of work algorithm have several consequences because of using more and more processing device to increase chance to get reward, firstly extremely high energy consumption which also leads to other environment problems such as high amount of carbon footprint and electronic waste. It is estimated that Bitcoin's energy consumption is just lower than 38 countries which means bitcoin use more energy than rest of any countries. In addition to that annual carbon footprint of all bitcoin related process is close to New Zeeland which is a country having 4.8 million people on it (Digiconomist, n.d.). These are important numbers that should be considered. Investing to bitcoin increase demand that increasing price that increasing demand again and attract more miner that increase processing power and all these harmful consequences. In future maybe some people or government start a campaign or convince people to use other coins or release a patch to update coin to solve these problems. Probably natural consequences are the most important disadvantage of Bitcoin. Second result of upward trend and increasing process power is since network's whole processing power increased, individual's chance decreased to mine successfully. So, people formed pools that allow more than one person to bring together their processing power to increase their chance to mine, then share reward according to individual's processing power. In fact, this tool decreases network's decentralization. For example, here is 23-27 December 2020 distribution of blocks mined to miners and pools in (Figure 1.1). As it seems some of the pools can come together and gain control of the network by their processing power but this would make bitcoin's reputation and price collapse and it is unlikely since this would be like killing chicken which gives golden egg.

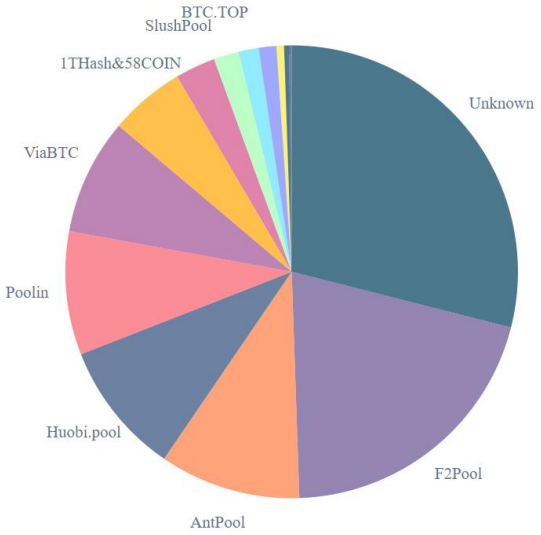


Figure 1.1 source: https://www.blockchain.com/en/pools

Table 1 Source: https://bitinfocharts.com/bitcoin/

Block Information	
Average Block Adding Time:	497s (8 m 17sn)
Block Size (limit):	892 KB (1 MB)
Block Reward:	6.25 BTC

Table 2 Source: https://coinmarketcap.com/, https://bitinfocharts.com/bitcoin/

Situation by December 27/12/2020	
Price:	≈ 27,000.00 $
Market Cap:	≈ 500,000,000,000 $
Volume:	≈ 65,569,418,136 $ (2,442,420 BTC)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 18,582,618 BTC (21,000,000 BTC), (%88.5)
One Month Change:	≈ % +58
Bitcoin Dominance:	≈ % 70
Average Fee per Transaction:	≈ 7 $

As it seems bitcoin has a limit of supply and circulation supply is almost ninety percent of it. At the beginning there was 0 bitcoin when first block was written. Then all this circulation supply is provided to market by miners when they rewarded. This situation makes some people confused because they think this cause inflation (giving money to the market by time) but, for example in 2021 approximately 50.000 block will be mined (one per ten minute) and 312500 BTC will emerge which is %1.6 of current supply. On the other hand, for example Eurozone economies also increased their money supply in 2019 by %2.6 (ceicdata, n.d.). As conclusion, if Bitcoin has inflation because of increased supply, non-digital currencies' supply increases by time, too. Other indexes indicate different results, too. For example, Bitcoin has significant market cap, in fact if

it were a company it would be in the most capitalized 15 company in the world, have higher market cap than companies like visa and Samsung (companies, n.d.) that indicates how much money, so people, interested in. Another supporting data for people's interest is, according to Nate Maddret (2020) who is a researcher at Coinmetrics in 2020 active Bitcoin addresses increased by %105 which indicates increasing interest and more trustful market. And this market cap's five percent is held by institutional corporations which emphasizes it is not only individuals but also institutional companies are interested in Bitcoin, too (Bitcoin Treasuries, n.d.).

Bitcoin dominance shows rate of money invested in bitcoin to money invested in all cryptocurrencies. It changed between %60 and %70 in 2020 (Coinmarketcap, n.d.). It is changed according to news. For example, if a company like PayPal or any other payment service company approves usage of Bitcoin dominance would increase because news about only bitcoin and this piece of news attracts people to buy bitcoin not any other altcoins. So, if market cap of all coins and bitcoin dominance increase it obviously causes rise of Bitcoin prices, too or if market cap all coins stays stable and bitcoin dominance increases, this means altcoin prices are going to decrease and Bitcoin price are going to increase. Probably in untrustful situations bitcoin dominance would increase because its market cap is higher and more trustful than other currencies so Bitcoin can behave as safe port like gold of digital currencies and its dominance increases.

Average fee for a transaction is approximately 7$ (BitInfoCharts (n.d.)) which is relatively high for Bitcoin's first aim. For instance, PayPal (2020) took maximum fee of 5$ for any transaction including international transactions. This makes Bitcoin non feasible to use for transaction based on blockchain technology but make it investible and holdable commodity.

Bitcoin is seen future's main currency by some people and they believe its prices will go even higher. Is this certain nobody knows but when any news about bitcoin will be accepted for payment or will be used by someone or something, are going to cause rise in Bitcoin prices.

Bitcoin Cash (BCH)

Bitcoin cash is a hard fork of Bitcoin blockchain which was created in August 2017 (Frankenfield, 2020). This hard fork includes a bigger block size which allows more transactions at the same time. This cryptocurrency gets another hard fork in November 2018 and split into Bitcoin Cash ABC and Bitcoin Cash SV or also known as Satoshi Vision (Frankenfield, 2020)

The differences between Bitcoin and Bitcoin Cash

According to Satoshi Nakamoto Bitcoin should be used as a peer to peer cryptocurrency which is for daily transactions (Nakamoto, 2008). After a while when it was becoming mainstream cryptocurrency and got more value it started to be seen as a kind of investment tool rather than a kind of currency. Bitcoin blockchain had some issues about scalability because the blockchain could not get over the increased number of transactions. Due to the fact that the transaction time and fees increased enormously. Actually, this was caused by the 1 MB block limitation of blockchain consensus (Frankenfield, 2020).

Bitcoin Cash consensus suggests that the increasing block limitation from 8 MB to 32 MB would be a solution for scalability problems like was mentioned. The average number of transactions per block on Bitcoin at the time Bitcoin Cash was proposed was between 1,000 and 1,500.4 The number of transactions on Bitcoin Cash's blockchain during a stress test in Sep. 2018 surged to 25,000 per block (Frankenfield, 2020).

Bitcoin Cash supporters like Roger Ver suggest that increased number block size is the real vision of Satoshi Nakamoto when the cryptocurrencies compete against big payment service companies such as Visa or MasterCard (Frankenfield, 2020).

Bitcoin Cash is also different from bitcoin in a different aspect. The Blockchain of Bitcoin Cash does not support Segregated Witness which is also known as SegWit (Frankenfield, 2020). SegWit retains only information or the metadata relating to a transaction in a block. Typically, all details pertaining to a transaction are stored in a block (Frankenfield, 2020).

Beside the ideological and technical differences Bitcoin and Bitcoin Cash have several similarities. Both of the cryptocurrencies use Proof of Work (PoW) and both of them share the services of Bitmain, the biggest cryptocurrency miner. The Supply of Bitcoin Cash is restricted at 21 million like Bitcoin. Also, like Bitcoin, Bitcoin Cash started on using Emergency Difficulty Adjustment (EDA) which is a kind of mining difficulty algorithm. EDA is a kind of algorithm that adjusts the mining difficulty in every 2016 block which is about a 2 weeks period (Frankenfield, 2020).

History of Bitcoin Cash

In 2010 an average Bitcoin block was less than 100 KB and the fee of a transaction was less than a couple of cents, so this situation made bitcoin blockchain vulnerable to some kind of attacks like consisting entirely of cheap transactions, that could potentially cripple the Bitcoin blockchain. To prevent these kinds of situations bitcoin's block size is restricted at 1 MB. Also, a time restriction was added to the bitcoin system which is allowed to one block in ten minutes. So, these restrictions added another security layer of Bitcoin blockchain (Frankenfield, 2020).

But those safeguards proved to be a hindrance when bitcoin gained mainstream traction on the back of greater awareness of its potential and enhancements to its platform (Frankenfield, 2020). In January 2015 average block size had increased to about 600K. Due to the fact that the approving time of a block has increased enormously. Because of that the system fee has increased, so this situation weakens the argument of Bitcoin as a competitor to an expensive credit card system (Frankenfield, 2020).

Developers proposed two solutions to this problem. One of them is increasing average block size or excluding some information of transactions to fit more data into one block. The developer team of Bitcoin whose name is Bitcoin Core did not consider the proposal to increase block size. Meanwhile, a new coin with resilient block size which was named Bitcoin Unlimited was hacked and struggled to gain attention because of its viability as a currency for daily transactions (Frankenfield, 2020).

In August 2017 Bitcoin Cash was launched and each bitcoin holder received an equivalent amount of Bitcoin Cash so because of that the coin number in the system doubled. Bitcoin Cash was listed at some of cryptocurrency exchange platforms at an impressive price of $900. But some of the biggest cryptocurrency platforms such as Coinbase and itBit boycotted Bitcoin Cash and did not allow listing Bitcoin Cash in their platform (Frankenfield, 2020). But Bitcoin Cash received a great support from Bitmain. Because of that, the supply of coins which was needed for cryptocurrency exchange ensured. In December 2017 Bitcoin Cash was traded about 4.091 dollars (Frankenfield, 2020).

Paradoxically enough, Bitcoin Cash itself underwent a fork slightly more than a year later due to the same reason it split from Bitcoin. Bitcoin Cash hard forked into Bitcoin Cash ABC and Bitcoin Cash SV in November 2018. This time the controversy was about the usage of smart contracts and its effect on average block size.

Craig Wright who claims that Satoshi Nakamoto is himself is led to Bitcoin Cash SV. He refused to use smart contracts on a platform which should be a payment method. The drama prior to the latest hard fork was similar to the one before forking Bitcoin Cash from Bitcoin in 2017 (Frankenfield, 2020). Due to the hard fork more funds have flowed into the cryptocurrency ecosystem. Both of the cryptocurrencies achieved respectable values at crypto exchange.

Table 3 Source: https://bitinfocharts.com/bitcoin%20cash/

Block Information	
Average Block Adding Time:	670s (11 m 10s)
Average Block Size (limit):	314 KB (8 MB)
Block Reward:	6.25 BCH

Table 4 Source: https://coinmarketcap.com/currencies/bitcoin-cash/, https://bitinfocharts.com/bitcoin%20cash/

Situation by December 27/12/2020	
Price:	≈ 335.00 $
Market Cap:	≈ 6,236,525,000 $ #8
Volume:	≈ 7,057,534,742 $ (20,880,280 BCH)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 18,582,618 BCH (21,000,000 BCH), (%88.5)
One Month Change:	≈ % +28
Average Fee per Transaction:	≈ 0.004 $

Concerns About Bitcoin Cash

Several improvements over Bitcoin Cash predecessor were promised by the Bitcoin Cash team. But none of them have been delivered yet.

The most important promise was about block size. Bitcoin Cash's average block size is very less than Bitcoin average block size. The smaller block size indicates that Bitcoin Cash's main thesis of allowing more transactions with the help of larger blocks is not tested yet. Also, Bitcoin's fees have dropped enormously, making it more competitive against Bitcoin Cash for daily life transactions.

Other cryptocurrencies which have similar aim to becoming a cryptocurrency for daily usage have announced some partnerships with governments and companies at home and abroad for instance Dash, Litecoin etc.

The second hard fork also indicates problems of managing the Bitcoin Cash developer community. A big part of the community believes that Bitcoin Cash's original vision diluted, so this situation can lead to another fork in the chain. Smart contracts are an essential feature of blockchains however it is not certain that Bitcoin Cash will be a platform for smart contracts or simple daily payment system (Frankenfield, 2020). Beside all this Bitcoin cash does not have a clear managing protocol. While other cryptocurrencies, such as Dash and VeChain, have innovated and outlined detailed governance protocols that assign voting rights, the development

and design of Bitcoin Cash seem to be centralized with its development teams (Frankenfield, 2020). So this creates unclarity in the minds of Bitcoin Cash investors.

Bitcoin SV

History

Bitcoin SV (Satoshi Vision) is emerged as a result of, a conflict in Bitcoin Cash network. it is hard fork of Bitcoin Cash so Bitcoin. After bitcoin cash emerged, a new conflict emerged between Bitcoin Cash community. One side of conflict wanted to stay at 32 MB blocks and also implement new technical protocols to make blockchain more anonymous which are deviation from Satoshi's Vision according to other side of conflict. This led to emerge of new fork which is stated that it is following Satoshi Nakatomo's first vision mentioned in Bitcoin Whitepaper by its supporters. This process is called as "Hash War" and date of emergence of Bitcoin SV (12 November 2018) fork is called as "Bitcoin Independence Day" by its followers. Afterwards of this event is called "Application Wars". Application wars describes the race between developers and businesses to create applications, which are better than applications on Bitcoin, Bitcoin Cash and other networks, on Bitcoin SV blockchain. In 2020, developers planned and implemented a Genesis Update in February, their aim was getting close to Satoshi's original ideas as much as possible and stabilizing network. In addition to that new update also covered scaling issue and made developing applications easier by reenabling the Bitcoin script language (Bitcoin SV, n.d.). Probably related with these developments BSV token's price rose up almost %200 in January 2020 but it should be noted that since Bitcoin SV is a fork of Bitcoin and it held some main features of Bitcoin like supply limit, block mining time, block reward system and halving, in 2020 Bitcoin SV also had halving and this could cause rise up, too.

Features

a) Stability

b) Scalability

c) Security

d) Safe Instant Transactions

Stability

According to BSV (n.d.) community stability is key feature for businesses, which is a valid consumer to use Bitcoin SV network according to community. So, community claims that Bitcoin SV is a stable network that is provided by controlled and well known structure to get close to original Bitcoin Protocol, allow developments in itself while network stays stable. Structure of Blockchain network allows different concepts like smart contract, tokenization, atomic swaps etc.

Scalability

Developers' aim is making Bitcoin SV an accepted payment platform, so they are aware that to do this network must carry high volume of transaction. As its prior reason to be new fork, first of all Bitcoin SV network have focus on increasing this capacity by increasing standard block size and making it flexible and increasing performance. They use a system called SV Gigablock Testnet (SV-GBTN) which fixes demand and performance balance (Bitcoin SV, n.d.).

Increased blocks make Mining more profitable because total transaction fee increases, also make transactions cheaper because more transactions allowed in one block make transactions faster, so even people don't pay much fee, their queue comes earlier.

Also, Bitcoin SV community claims that (n.d.) this increased scaling attract businesses more than lower block size because enterprise's applications need larger blocks with larger capacity.

Security

Bitcoin SV community (Bitcoin SV, n.d.) know that they have to prepare network to be a world currency and to achieve this security is one of the most important aspect. Network uses Quality Assurance. This provides testing stages that check validity of project with. Developers' claims as a result of this, it makes sense to use Bitcoin SV in important areas like medicine and national security. This process work in three steps including QA processes with security experts, blockchain security company and a contest to find bugs organized as find bug and take reward system.

Safe Instant Transactions (SIT)

Developers (Bitcoin SV, n.d.) see SIT as a brick and mortar to become a global payment system and they claim they focus on improvements in this area, too.

Table 5 Source: https://bitinfocharts.com/bitcoin%20sv/

Block Information	
Average Block Adding Time:	576s (9m 36sn)
Average Block Size (limit):	852 KB (no limit)

Block Reward:	6.25 BSV

Table 1 Source: coinmarketcap.com, https://bitinfocharts.com/bitcoin%20sv/

Situation by December 27/12/2020

Price:	≈ 165.00 $
Market Cap:	≈ 3,000,000,000 $ #13.
Volume:	≈738,850,000 $ (3,250,000 BSV)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 18,200,000 BSV (21,000,000 BSV), (%86.6)
One Month Change:	≈ % +3
Average Fee per Transaction	≈ 0.0003 $

On paper, Bitcoin SV provides lots of things, low transaction fee, profit for miner, stability, security so on but its price is lower than half of Bitcoin Cash which is seem requiring updates by Bitcoin SV's creators. Maybe it is because people do not trust Craig Wright who is an important figure for Bitcoin SV and claims he is Satoshi Nakamoto (coindesk, n.d.). But this network is not a centralized structure and even if it was, people trust Bitcoin that is created by completely pseudonymous Satoshi Nakatomo, so why not Bitcoin SV. Its Market Cap is nothing in contrast to Bitcoin but any of altcoins is not even close to Bitcoin, and Bitcoin SV has highest nineth market cap which is not so low. Its circulation supply is not much different from Bitcoin, eventually it is a fork of Bitcoin.

Bitcoin SV has a good potential to be global payment system with its scalability, low transaction fee and relatively high market cap. But by December 2020 it is not even bought or sold in Binance which is one of the biggest coin market. In future, if Binance accept Bitcoin SV in its market, this would likely make its price increase or any corporation start to approve Bitcoin SV as payment or investible currency, this also cause rise in its value like every cryptocurrency. On the other hand, if people's perception about cryptocurrencies change and people starts to trust and use cryptocurrencies more, Bitcoin SV is highly attractive to use as transaction currency because of low transaction fees, scalable and large blocks which can adapt changed demands and its good position in market cap order.

Litecoin (LTC)

Litecoin is measured by market capitalization which means the amount of currency on the market is the fourth largest cryptocurrency (Coin360, n.d.). Litecoin can be considered as a kind of daily payment system.

How was Litecoin created?

Like most of the cryptocurrencies Litecoin is not created by the government which historically has been seen as the creator of the currencies. Litecoin is created by the elaborate procedure called mining which a society joins to the system voluntarily. Unlike traditional currencies the supply of Litecoin is limited to only 84 million Litecoin. As opposed to 10 minutes block time of bitcoin Litecoin's block is about 2.5 minutes (Mcfarlane, 2019).

Mining for Litecoin

Litecoin's block reward is 12.5 Litecoin and on 24 August 2023 the reward will be halved like previous halving events which happens in 4 years of periods. Like most of the Proof of Work Cryptocurrencies miners need hardware products which are mostly specialized to do mining. The greater machine capacity for mining leads to a better chance to earn block rewards (Mcfarlane, 2019).

What Is Litecoin Worth?

Any currency's value (Can be fiat or gold does not matter.) is valued by society actually. If the Federal Reserve releases a lot of money to market the money's value drop in a short time. This phenomenon transcends currency (Mcfarlane, 2019). If any commodity or service becomes more available this leads to cheaper prices for them (Mcfarlane, 2019). The creators of litecoin understood from the start that it would be difficult for a new currency to develop a reputation in the marketplace. But by restricting the number of litecoins in circulation, the founders could at least allay people's fears of overproduction (Mcfarlane, 2019).

Litecoin has some advantages on Bitcoin. Less block time provides fast and more transactions in the same amount of time. Also, Litecoin has a little fee when compared to bitcoin and PayPal. Litecoin's inherent scarcity makes hyperinflation impossible, but there's still the challenge of garnering general acceptance and getting more people to use the currency (Mcfarlane, 2019).

Table 6 Source: https://bitinfocharts.com/litecoin/

Block Information	
Average Block Adding Time:	144sn (2m 2sn)
Average Block Size (limit):	45 KB (1MB)
Block Reward:	12.5 LTC

Table 6 Source: coinmarketcap.com, https://bitinfocharts.com/litecoin/

Situation by 06/01/2021	
Price:	≈ 130.00 $
Market Cap:	≈ 10,934,174,770 $ #4
Volume:	≈10.000,000,000 $ (61,000,000 LTC)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 66,245,618 LTC (84,000,000 LTC), (%70.4)
One Month Change:	≈ % +90
Average Fee per Transaction:	≈ 0.042 $

Ethereum (ETH)

Ethereum which was introduced in 2015 is an open source, blockchain based, decentralized app platform which is using ether cryptocurrency for sustainability. Ethereum allows creating Smart Contracts and Decentralized Apps on its blockchain without any control, fraud, downtime or interference from a third party (Frankenfield, 2020). It is not just a platform it is also a programming language which can work on its blockchain system. It allows developing and publishing distributed apps.

How can Ethereum work?

Ethereum apps work on a cryptographic token which is called ether. Ethereum Foundation started an early sale for ether which received a big demand. Ether is a kind of tool to develop decentralized apps on Ethereum Blockchain. Due to the fact that ether is mostly used for digital currency like other cryptocurrencies, and it is used inside Ethereum to run applications.

According to the Ethereum Foundation it can be used about everything (Frankenfield, 2020). Ethereum's one of the biggest projects is Microsoft's partnership between ConsenSys. Microsoft offers a kind of "Ethereum Blockchain as a Service" (EBaaS) on its Azure Cloud Services. This service allows enterprises and developers to have a single click blockchain developer environment (Frankenfield, 2020).

Ethereum Classic and Ethereum

Ethereum blockchain separated into two different blockchains, Ethereum and Ethereum Classic. After a malicious actor stole more than $50 million worth of funds which had been raised on the DAO, a set of smart contracts originating from Ethereum's software platform (Frankenfield, 2020). New Ethereum was a hard fork from original software to inhibit new malware attacks.

Ether (Cryptocurrency)

Ether is a transferable token that sustain operations on Ethereum blockchain. It is a tool that allows network participants to execute their requests on the blockchain, so it is an encouraging instrument for the sustainability of the chain (Kenton, 2020).

Understanding Ether Cryptocurrency

Commercial and individual usage of Ethereum is allowed. Ethereum developers need to pay fees to the blockchain to execute their own code on the Ethereum blockchain. Executing an app which

needs minimal usage of network resources will be cheaper than other apps which need more network resources.

Ether as a "Fuel"

Ether can be considered as a fuel of the Ethereum network. Ether's function as a way of tracking and facilitating transactions is metaphorically closer to a fuel rather than a currency (Kenton, 2020).

Ethereum network calculates how much fees are required for execution of a smart contract and charges it to the developer. Like an inefficient engine will require more fuel, and an efficient engine will consume less fuel, data-hungry apps require more ether to process transactions (Kenton, 2020). This system is very different from other standard cryptocurrencies.

Ether as a Cryptocurrency

Ether's supply is restricted at 18 million ethers yearly. Before 2014 60 million ethers were created and given to developers who contributed the Ethereum blockchain. Another 12 million ether was created for the Ethereum Foundation Fund (Kenton, 2020).

Conversely, Ether does not have an absolute cap like Bitcoin. Right now creation of a block is about 15 seconds long and every creation of a block 5 ether enters the market as a reward of miners. Sometimes another miner can create a different block in that time that miner gets 2-3 ether and the block which the second miner created is called uncle block (Kenton, 2020). However, the new blocks from the chain of the uncle block are not allowed to get reward.

Ethereum Developments and its effects to Ether

Ethereum developers working to move the network to proof-of-stake (PoS) from 2017. This is called "Project Casper" and its effects would be enormous on the chain. Ethereum developers deployed the Istanbul hard fork, and it decreases block processing time in late 2019. Pedro Febrero suggests that because of this hard fork developers not tweaking the difficulty of mining new blocks to fit the update.

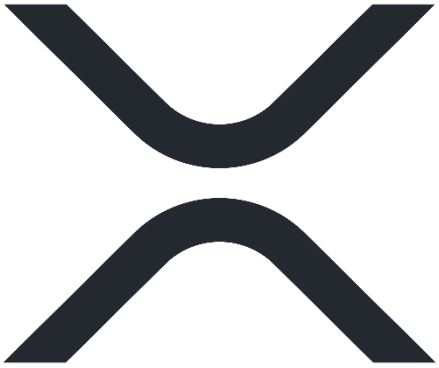
At block number 9,200,000 the Muir Glacier upgrade was released which delays the difficulty bomb for another 4 million blocks. Anna Larsen put forward that this upgrade improved the performance of the Ethereum blockchain but increased ether inflation about 5%. Due to the fact that Ethereum project's trust has eroded.

Table 7 Source: https://bitinfocharts.com/ethereum/

Block Information	
Average Block Adding Time:	13sn
Average Block Size:	43 KB
Average Block Revenue:	3.5 ETH

Table 6 Source: coinmarketcap.com, https://bitinfocharts.com/ethereum/

Situation by 06/01/2021	
Price:	≈ 1147.00 $
Market Cap:	≈ 130,994,161,505$ #2
Volume:	≈ 40,280,000,000 $ (35,170,000 ETH)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 114,138,433 ETH (no limit), (%70.4)
One Month Change:	≈ % +83
Average Fee:	≈ 8.86 $



Ripple (XRP)

XRP is a digital asset created to provide payments. It was established in 2012 and XRP is an open source, permission less and decentralized blockchain technology. XRP processes transactions in three or five seconds. XRP, which does not have a centralized system, can be sent directly. It is an instrument that can transfer different currencies quickly and efficiently (*Ripple*, n.d.). Market value of XRP is $ 9.9 billion. This makes it the fourth largest cryptocurrency among cryptocurrencies. XRP was created by the Ripple company as a competitor to other digital assets and monetary payment platforms such as SWIFT. XRP works this way: XRP Ledger processes transactions approximately every three or five seconds or when independent validator nodes reach a consensus on both the order and validity of XRP transactions, as opposed to proof-of-work mining like Bitcoin. It is possible for anyone to become a Ripple validator, and the list currently consists of universities, financial institutions and Ripple company. There are more than

forty-five billion tokens in circulation. Ripple had an all-time high of $ 2,7704 in January 2018 (coinmarketcap, n.d.).

The advantages of XRP over other cryptocurrencies are as follows:
Widespread Usage
Fast
Scalable
Decentralized Remittance System
Stability
Eco-friendly

Widespread Usage
While there are more than two thousand altcoins in circulation, Ripple has been accepted by over 100 companies and banks worldwide and cooperates in money transfers to them. Ripple, which gained widespread use thanks to this cooperation, attracted the attention of many investors. It also contributes to its legitimacy and increased value, thanks to its easy acceptance by financial institutions (Tiwari, 2020).

Fast
Delayed transactions can lead to fraud and will lose faith in the system. XRP allows you to complete a transaction in approximately 3 seconds. In traditional systems, these processes are longer and may even make you wait for days. XRP is a precise, fast, secure and global way to make transactions (Tiwari, 2020).

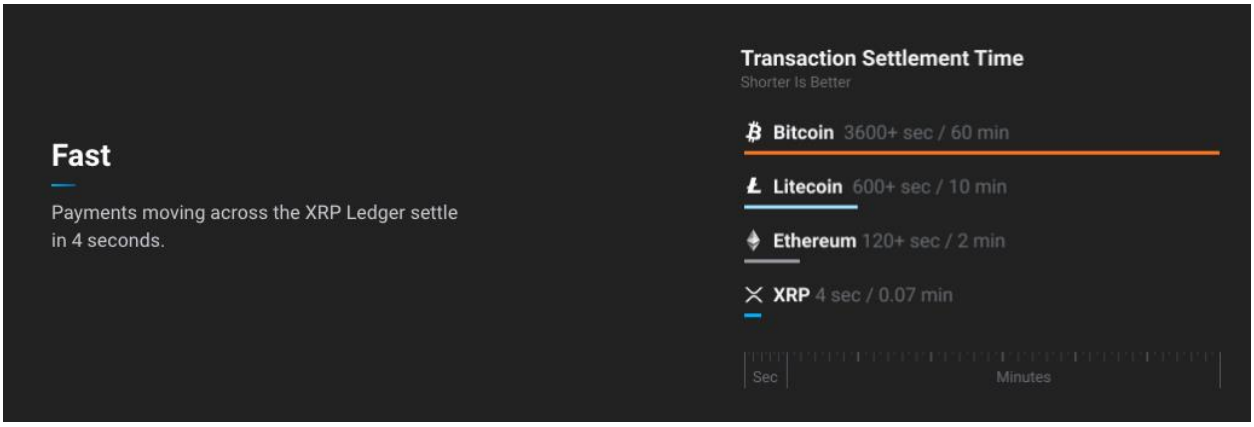


Figure 1.1 source: https://ripple.com/xrp/

Scalable
The strength of a system is directly proportional to its ability to serve the market. XRP can handle more than 1,500 transactions per minute with a high degree of accuracy and consistency.

Managing the same volume of business as some of the largest financial systems used with VISA is scalable (*Ripple,* n.d.).

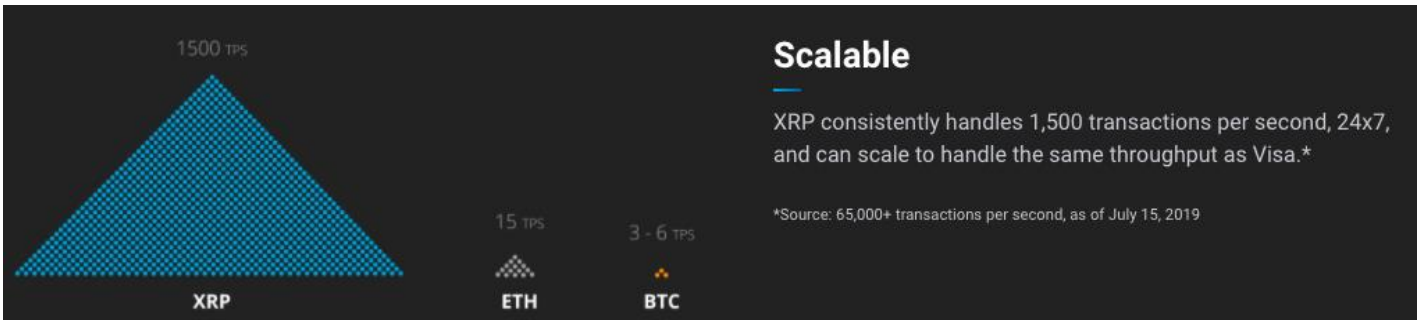


Figure 1.2 source: https://ripple.com/xrp/

Decentralized Remittance System

Ripple is built with open-source technology. The group of validators is growing day by day and has access to different markets and platforms (Tiwari, 2020).

Stability

Cryptocurrencies are currencies with high volatility and the risk is high. But Ripple differs from other cryptocurrencies in the market in this regard. Since its foundation in 2012, it has steadily grown and added value to its investors' investments. In this way, he convinced institutions to invest in XRP (Tiwari, 2020).

Eco-friendly

XRP Ledger is not a proof-of-work protocol unlike Bitcoin. There is no mining. In other words, it performs XRP transactions instantly without energy costs (*Ripple,* n.d.).

XRP has a major disadvantage. Recent news that has had a very negative impact on XRP is as follows: The US Securities and Exchange Commission (SEC) released a press release on December 22, Ripple Labs Inc. and against the company's two executives, Christian Larsen and Bradley Garlinghouse. The US Securities and Exchange Commission (SEC) claimed that Ripple Labs Inc, Larsen, and Garlinghouse raised over $ 1.3 billion through an unrecorded digital securities offer. The US Securities and Exchange Commission suggests that digital assets known as XRP are raising funds by selling them informally to investors in the US and around the world. The document also alleges that Ripple has distributed billions of XRP in exchange for non-cash charges such as labor and market-making services. In short, Ripple paid for human services in XRP instead of traditional currency (Harper, 2020). The outcome of this lawsuit is very important for XRP's presence in America. Besides this disadvantage, although the main purpose of the Ripple network is to make cross-border money transfers very quickly and at low cost, just like swift; Very few banks in the world have launched XRP transactions. Most banks are still

working with XRP in the testing phase. Another criticism is that the RippleNet presses the price downward by selling the high amount of XRPs in its possession from time to time. This creates a contrasting perception with the decentralization phenomenon that underlies cryptocurrencies.

Table 6 Source: coinmarketcap.com, https://bitinfocharts.com/xrp/

Situation by 06/01/2021	
Price:	≈ 0.232 $
Market Cap:	≈ 10,216,647,833 $ #5
Volume:	≈ 5,430,000,000 $ (23,520,000,000 XRP)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 45,404,028,640 XRP (100,000,000,000), (%45.4)
One Month Change:	≈ % - 61

Binance Coin (BNB)

Binance Coin (BNB) is a cryptocurrency created by the Binance cryptocurrency exchange. Binance Coin (BNB) was launched as an ERC-20 based cryptocurrency, but later Binance set up its own chain and migrated to a BEP2 based infrastructure. Existing ERC20 tokens are burned into BEP2 tokens. Binance, one of the largest exchanges in the world with its volume, has shown a significant increase in the volume and value of the Binance Coin (BNB) crypto currency against real money in proportion to the stock market volume. Binance Coin (BNB) was first launched with an ICO (Initial Coin Offer) held between June 26 - July 3, 2017. A total of 100,000,000 BNB was released at the first launch (Binance Academy, n.d.).
When it was first offered, 1 BNB was worth about $ 0.11 and is now worth much more in real money. January 3, 2021 instant price is $ 38. The market volume is currently US $ 5.496 billion. It is the eighth highest cryptocurrency by market capitalization. There is a total of 144,407,713 BNB in the market (coinmarketcap, n.d.).

Figure 1.1 source: https://coinmarketcap.com/currencies/binance-coin/

Binance exchange buys Binance Coin (BNB) with 20% of its annual profit and burns the BNB coins it bought. This transaction will continue to 100,000,000 BNB remaining in the market. The purpose of this transaction is to prevent inflation in the Binance Coin (BNB) market. It is possible to buy / sell between Binance Coin (BNB) and crypto currencies on the Binance exchange. The most important advantage of Binance Coin is the commission discount on the Binance exchange (Binance Academy, n.d.).

With Binance Coin (BNB), you can pay commission on buying / selling transactions on the Binance exchange. For payments made with Binance Coin (BNB), Binance offers a discount of 50% in the first year, 25% in the second year, 12.5% in the third year and 6.75% in the fourth year. Levels are given according to the amount of BNB the user holds and the total volume made. Binance Coin (BNB) is a non-mining cryptocurrency. The entire Binance Coin (BNB) amount was produced by the Binance exchange on the first day, half of which was sold to cryptocurrency investors. (Binance Academy, n.d.).

Privacy-Oriented Coins

Monero (XMR)

Monero is a privacy concerning cryptocurrency which based on Blockchain and it uses Proof of Work algorithm. Its root goes to another blockchain in 2012 named Bytecoin. Base technology of Bytecoin was CryptoNote which is used by other privacy-oriented cryptocurrencies, too (Aaron, 2020). In 2014, a group of seven developer, who are five of anonymous and two of known, forked Bytecoin and launched Bitmonero which will change as just Monero in future (getmonero, n.d.).

Monero's philosophy is providing private transactions to its customer. In contrast to common knowledge Bitcoin and most of the altcoins do not provide their services to customers which make customer completely anonymous or untraceable. Monero's aim is providing these features to Monero users.

Monero Blockhain has built on three main value: Security, Privacy, Decentralization (getmonero, n.d.).

Security

Monero users can trust what they do with Monero. There must be no doubt for getting error or be attacked. Network ensure this trust by giving miners enough reward who are responsible to make users feel secure and also ensure this trust by their technology using new and secure cryptology methods (getmonero, n.d.).

Privacy

What makes Monero Monero is its privacy. Monero claims it provide its users privacy in their transactions and make privacy a default and not changeable feature on network. And Monero provide this to every people who is aware or not aware of how technological stuff work. This privacy allows their users to hide their spends from any other third party (getmonero, n.d.).

Decentralization

Monero community wants to make Monero network decentralized as much as possible. People must trust to network which does not include any trusted third party. Monero uses anti-ASIC technology to avoid make some nodes more powerful. In addition to that Monero's Proof of Work algorithm makes mining in standard computers facilitating decentralization (getmonero, n.d.).

How Monero Provide These Features:

Privacy

Spend Key: All accounts have Spend Key that is used while sending transactions. It is used to sign transactions.

View Key: All accounts have View Key and it is used to see transactions related with this account. Account owner can share this key with any other person and allow him to see owner's transactions (getmonero, n.d.). This makes Monero optionally transparent. (Monero addresses were created by using view and spend keys)

Ring Signature: This feature is used to hide sender's address (getmonero, n.d.). While user sends Monero to receiver, transaction is not signed by sender but also another randomly selected addresses from network. This algorithm makes sender's address hidden because any observer cannot see which one of the signatures are belong to sender.

Key Image: As a result of Ring Signatures, it is not possible to check sender of a transaction, so this can lead to double spending. Key Images are used to here. Every transaction has a unique single Key Image which prevent to spend same Monero twice (getmonero, n.d).

Stealth Addresses: To ensure receiver received transaction anonymously Steatlh Addresses are used by Monero Network. While sender sending Monero, a new temporary address is created and transaction goes to this address. Then, receiver search network by using its view key to search are there any transaction sent to himself and took it. As a result of this algorithm, any observer cannot relate a connection between sender and receiver. On the other hand, if sender needs to prove that he sent Monero, he can prove it by his spend key (getmonero, n.d.).

Ring CT (Ring Confidential Transactions): Ring CT was developed by Shen Noether. Ring CT algorithm started to be used in Monero network in January 2017 and Ring CT is used to hide transaction amount, before Ring CT launched observer could see transaction amounts. After launch, senders started to not share transaction amount but they commit it which gives an proof that sum of inputs of transaction is equal to sum of outputs of transaction, otherwise people could exploit this privacy and make money from nothing. Used commitment is Pedersen Commitment which allow users to prove transaction is valid without sharing private transaction data (getmonero, n.d.).

Although these algorithms it is still possible to find address owners identity by tracing their IP. To solve this problem a project named "Kovri" is proposed. It was going to be alternative to Tor Browser which make IP's untraceable for anonymity. But project failed (gitlab, 2019). It could increase trust and encourage usage of Monero and could affect its

price. If something similar is considered to implement to network, it would certainly affect Monero's price.

Decentralization

Mining: Monero uses a Proof of Work algorithm which is a type of CryptoNight and uses RandomX (getmonero, n.d.) algorithm that makes network ASIC resistant to increase decentralization by executing random code and using techniques related memory. This also leads to better block reward distribution to avoid emergence of pools which are threads for decentralization (getmonero, n.d.). However, pools have significant control over network, biggest two pools mined more than half of last 1000 block by 31.12.2020 (https://miningpoolstats.stream/monero).

Smart Mining: Smart Mining's aim is making computers stay stable and making them work longer times and providing decentralization to network by providing higher number of participants to network. But smart mining reduces processing power of a device, so it is optional (getmonero, n.d.).

Open Source: Monero is an open-source project and has more than 250 developers (Github, n.d.).

Table 7 Source: https://bitinfocharts.com/monero/

Block Information (by December 31/12/2020)	
Average Block Adding Time:	125s (2 m s)
Block Size:	68 KB (changes according to demand)
Average Block Revenue:	1.23 XMR

Table 8 Source: https://coinmarketcap.com/currencies/monero/, https://bitinfocharts.com/monero/

Situation (by December 31/12/2020)	
Price:	≈ 157.00 $
Market Cap:	≈ 2,800,000,000 $ #14.
Volume:	≈940,000,000 $ (5,976,290 XMR)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 17,800,700 XMR (no limit)
One Month Change:	≈ % +24
Average Fee per Transaction:	≈ 0.033 $

Monero promising untraceable, private, secure and decentralized cryptocurrency. But this is something that governments do not want to see and governments are going to try trace this blockchain. In fact, USA government already tried. Internal Revenue Service (IRS) are ready to pay 1 million $ to developers who can develop a technology to trace Monero (Franceschi-Bicchierai, 2020). Government has point, this privacy can allow illegal situations but whatever they do, there are going to be a new developer who can find new ways to get rid of government pressure as Spagni said who is a developer of Monero (coindesk, 2020). In addition to that, most likely these new ways will serve to people who really have something to hide. So, these regulations and effort will only take this service from ordinary people. In addition to IRS, Financial Crimes Enforcement Network (FinCEN) also wants to regulate and trace Cryptocurrencies by demanding them transaction information. (US Department of The Treasury, 2020) On the other side, crypto community has also their proposal. "Anti-Money Laundering Regulation of Privacy-Enabling Cryptocurrencies" is published by Dana V. Syracuse, Joshua L Boehm and Nick Lundgren (2020) claiming without compromising privacy features, cryptocurrencies can be regulated against money laundering. Time will show what will governments' attitude against those currencies.

One of the biggest advantages of Monero is its "Fungibility" resulted from its untraceable feature. Since nobody can see past of Monero coins, all Monero coins have same value in contrast to transparent currencies. Since maybe some people do not accept coins which have involved some undesirable situations, these coin's value become lower than other coins of same blockchain. Monero's this feature probably increases user's intent to buy since this makes Monero closer to cash and increases trust to every Monero. Another advantage of Monero is flexible block sizes. This means in future if users, so transaction number increases, Monero can handle this situation without updates.

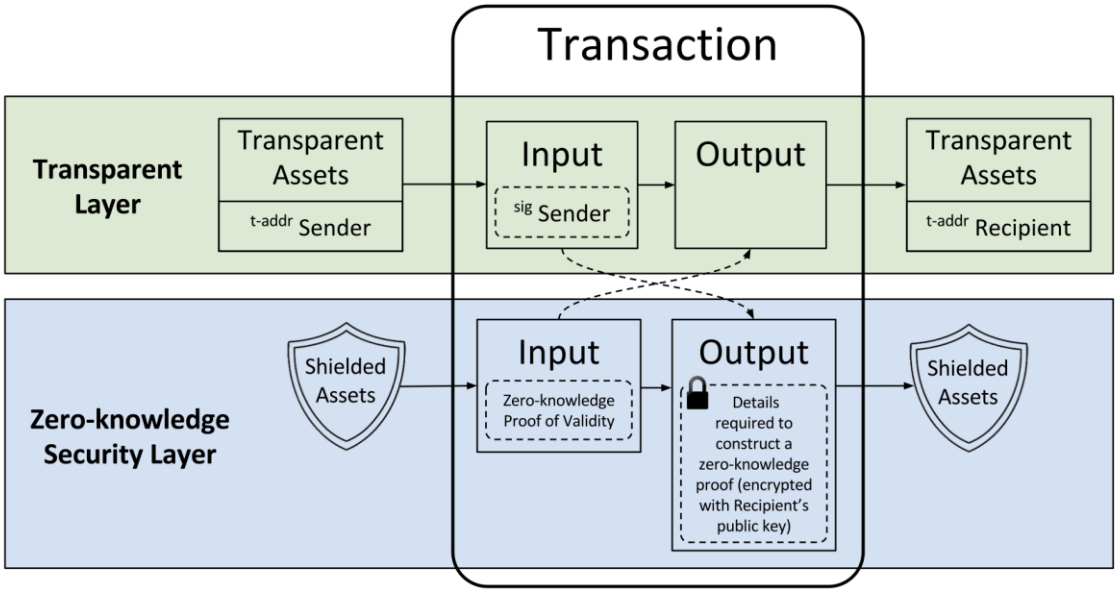
Zcash (ZEC)

Most conversations in the cryptocurrency sector mostly start and end with the Bitcoin topic. But the first cryptocurrency has some disadvantages. Beside its high fee rates it has some

fundamental privacy issues. The idea of a public and transparent blockchain is attractive but on the other hand it has some big problems about the modern concept of privacy. The open usage of blockchain can be used to detect illegal activities such as money laundering in opposition to this situation can create some problems for users (Sharma, 2018). For instance, a transaction which is related to tax can be seen on the open blockchain and this can lead to reveal of the user's personal data. Likely business-related transactions which are private on public blockchains could lead to some leaks (Sharma, 2018).

Zooko Wilcox who is the founder and CEO of Zcash claims that "Zcash is a new blockchain and cryptocurrency which allows private transactions (and generally private data) in a public blockchain. This allows businesses, consumers, and new apps to control who gets to see the details of their transactions, even while using a global, permissionless blockchain." (Sharma, 2018). Zcash is a privacy-oriented cryptocurrency that was developed in response to Bitcoin's problems. The blockchain of Zcash uses the same algorithm as bitcoin use but Zcash developers developed some improvements which allows semi-transparent processing on the chain. This means that the Zcash blockchain avoids radical transparency of bitcoin's blockchain. These improvements reveal user transaction data selectively.

Zcash's history lies in a cryptocurrency project which is called Zerocoin developed in the 1980s. Zerocoin was developed by Matthew Green who is a professor at Johns Hopkins University right now. For more information about Matthew Green you can look at his Johns Hopkins University website: https://isi.jhu.edu/~mgreen/. Back then, he was a graduate student at the institution. Zerocoin developed a system that called zero-knowledge proofs in order to conduct blockchain transactions. The proofs provided that the content of the transaction stayed anonymous even as the transaction can be seen publicly on the decentralized chain (Sharma, 2018). But implementation has some disadvantages, and they are elaborated on the Zcash white paper (Ben-Sasson et al., 2014). The first one is the heavy nature of calculations and its effect on the CPUs. Zerocoin transactions were about 45 k and to be accepted on the chain 45 ms was needed. The paper's author indicates that "The entailed costs are higher by orders of magnitude than those in bitcoin and can seriously tax a bitcoin network operating at normal scale," (Ben-Sasson et al., 2014). Secondly the implementation of zerocoin restricted functionality. For instance the system did not transmit an exact value. Users restricted transmitting fixed values determined by the system. Furthermore, the system had no native cryptocurrency and did not hide the metadata such as transaction amount and date on the ledger.



(Blockwolf, n.d.)

Zcash developers suggest that for short and effective verification zk-SNARK is needed, so they used the zk-SNARK algorithm in their Zcash project. The proof allows the transaction to happen without giving the information. Due to the fact that Zcash transactions can happen like Bitcoin without sacrificing anonymity (Sharma, 2018).

Another feature of Zcash is the changeability of the tokens. To put it more clearly all parties of the network allow all the ZCash coins as without considering its transaction history. In fully public blockchains such a special feature is impossible because the system allows blacklisting some tokens because of its transaction history. In this point of view Zcash is more likely to present cash. It is very hard to determine the old owners of the cash.

What Is zk-SNARK?

Zk-SNARK is an acronym that stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge.". A zk-SNARK will be evidence that permits you to quit offering on that one party with substantiation. It possesses certain data without uncovering that majority of the data. This evidence may be settled on could reasonably be expected utilizing a mystery enter made preceding the transaction takes out.

At the beginning for most of the cryptocurrency members privacy was one of the most important terms for the market. But privacy was always at the second place when the cryptocurrencies were trying to create a "trustless" system which guaranteed the integrity of the electronic cash. Bitcoin users assumed that their transactions were anonymous because their real identities are not related

to the public key of their wallet in the early 2010s. In spite of the fact that re-identifying people who had given pseudonymous data to multiple sources is not only possible it is also easy to do that (Peters, 2020). Because of some privacy issues which were mentioned before developers started to work on privacy-oriented coins such as Zcash which was backed by zk-SNARKs.

Zero-Knowledge Proof

The algorithm of zk-SNARK uses a technique which is named "zero-knowledge proof". The technical term's idea was developed in the 1980s. It is a kind of system that is a situation in which each of two parties in a transaction is able to verify to each other that they have a particular set of information, while at the same time not revealing what that information is. At least one of the two parties must have access to all the information for most of the other types of proof systems (Peters, 2020). A traditional proof can be associated with a daily used password to access any kind of social media account on the internet. The end user gives the password and the server checks the accuracy of the password. In order to do this servers must have the right to access the contents of the password. However, the zero-knowledge proof systems' algorithm allows the user to validate the password using mathematical proof without revealing the password itself.

The privacy and security advantages in this situation are clear: If the network does not have stored passwords then the password cannot be stolen.

The mathematical basis of zk-SNARKs is very complex. However, proof that mentioned allows one part of the network to show not only that part of information exists also shows that that part of the network has awareness of the information.

In the usage of the Zcash, zk-SNARKs algorithm can verify the information instantly and the algorithm does not require any interaction between the verifier and prover (Peters, 2020).

Weak Sides of zk-SNARKs

There are some concerns about zk-SNARKs. For example, if someone was able to access the private key that was used to create the parameters of the proof protocol, they could create false proofs that nonetheless looked valid to verifies (Peters, 2020). This explicitly allows a person to create new Zcash tokens. Zcash developers developed such a way as to make the proving protocols elaborate and spread out over multiple parties.

Zcash developers were created a 20% "tax" levied on all blocks created over the first years of the blockchain. This tax is named "the founder's tax" and it was used to pay the expenses of the cryptocurrency. The people who criticize Zcash put forward that the founder group can use this facet of the algorithm to create an infinite numbers of tokens and society can not be aware of the

existence of those tokens.Because of that it is impossible to know the exact number of Zcash tokens in existence right now.

Some developers have been working on an improvement of zk-SNARKs since 2019. This improvement includes removing the trusted set up. A team named Suterusu has developed a system called zK-ConSNARK that claims to be operable without a trusted set up which can provide privacy for mainstream cryptocurrencies such as Bitcoin (Peters, 2020).

The Applications of Zcash

The transparent and decentralized structure of cryptocurrencies create different applications for the end user. However, this situation creates problems with the traditional financial ecosystem. Its main reason is that the main aim of the traditional financial system is radical transparency so this leads to a controversy between traditional finance and privacy oriented cryptocurrencies. Due to the fact that Zcash suggests a solution called "zero-knowledge security layer" which is also known as ZSL. ZSL supports semi-transparent transactions. This kind of transaction allows the people to show some data of the transaction. Financial powerhouse JPMorgan Inc. (JPM) has already signed a partnership with Zcash to use its technology for Quorum which is an enterprise-ready distributed ledger, and smart contract platform. This illustrates that Zero Knowledge Proofs could be adopted on Wall Street and conventional finance (Sharma, 2018).

Zcash in the Markets

Zcash's genesis block was released on 28 October 2016 and is available for the trade from that time. The token is currently available for trading at cryptocurrency exchange platforms such as Huobi, Binance etc. During its launch, its price was about $4,293.37. But its price crashed by 98.8% within two months. Thanks to the support of some leading names like Edward Snowden Zcash's price rose up again (Sharma, 2018).

Recently one of the biggest cryptocurrency exchange platforms named Bittrex delisted Zcash and some other privacy-oriented coins from its services. This situation caused a big bear season on privacy-oriented coins. Nevertheless, Tyler Winklevoss who is the founding partner of one of the leading cryptocurrency platforms named Gemini said that they do not have any plans to delist Zcash on their platform. This was commented as a kind of support to Zcash (D, 2021).

Table 9 Source: https://bitinfocharts.com/zcash/

Block Information (by December 31/12/2020)	
Average Block Adding Time:	74s (1m 14s)
Block Size (limit):	15 KB (2 MB)

Block Reward:	6.25 ZEC

Table 10 Source: https://coinmarketcap.com/currencies/zcash/, https://bitinfocharts.com/zcash/

Situation (by December 31/12/2020)

Price:	≈ 62.00 $
Market Cap:	≈ 667,450,000 $ #45.
Volume:	≈ 752,000,000 $ (12,240,000 ZEC)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 10,850,000 ZEC (21,000,000) (%51)
One Month Change:	≈ % -24
Average Fee per Transaction:	≈ 0.03 $

DASH

Dash is a privacy digital currency that allows fast, simple and very low-cost payments anywhere in the world without the need for any central authority. It has a decentralized peer-to-peer network structure. Dash provides a secure payment method service thanks to its blockchain protected by strong cryptographic encryption techniques. Dash cryptocurrency was launched by Evan Duffield as "Xcoin" in January 2014. At that time, it changed its name as Darkcoin due to its frequent use in darknet markets. In 2015, it continued to its way with the name 'Dash', which stands for digital cash (Wheal, 2019).

Dash differs from many other Cryptocurrencies due to its low transaction fees and fast transfers. Dash also offers its users Instant send and private send options. Through Masternodes connected to the Dash network, users can make approved transfers within one or two seconds. Thanks to PrivateSend, which is another feature, privacy-oriented transfers that can only be followed by the sender and receiver can be performed in the Dash network. In the private send option, DASHs coming out of the sender wallet are mixed by Masternodes, made unmatched in the blockchain and delivered to the recipient's address. Only the sending and receiving wallets can follow this transfer (Wheal, 2019).

As with Bitcoin and blockchain, transactions on the DASH network are encrypted using a method called proof-of-work mining. Computers powerful in mining try to solve a difficult mathematical problem posed by the X11 hashing algorithm. Average block creation time is 2.5 minutes (dash, n.d.).

They promote their work on DASH official sites as follows:
"Anyone can participate in the network, and Dash is widely available for purchase around the world. The ingenious master node network means sending any sum of money around the world is as simple as tapping your phone at your local store to buy groceries. Say goodbye to slow transactions, complex international account numbers and high transaction fees – Dash is digital cash!" (dash, n.d.).

Table 11 Source: https://bitinfocharts.com/dash/

Block Information (by December 31/12/2020)	
Average Block Adding Time:	74s (1m 14s)
Block Size (limit):	34 KB (2 MB)
Average Block Revenue:	2.88 DASH

Table 12 Source: https://coinmarketcap.com/currencies/dash/, https://bitinfocharts.com/dash/

Situation (by January 03/01/2020)	
Price:	≈ 89.00 $
Market Cap:	≈ 880,012,462 $ #36
Volume:	≈ 979,779,502 $ (12,240,000 DASH)
Circulation Supply (Limit of the Supply), (%Rate):	≈ 9,900,000 DASH (18,900,000) (%52)
One Month Change:	≈ % -17
Average Fee per Transaction:	≈ 0.003 $

DASH, with a market value of $ 891 million, ranks thirty-sixth in volume among cryptocurrencies. The highest pricing it has seen in the market was $ 1493 in December 2017. On January 3, 2021, a DASH is $ 89. This is sixteen times less than his highest value he had seen before.

Figure 2.1 https://coinmarketcap.com/currencies/dash/

An important disadvantage that can be considered as a danger for privacy cryptocurrencies is the process of deleting cryptocurrencies from exchanges. Bittrex, one of the leading crypto currency exchanges in the market, is removing three privacy-focused coins from its platform. In the statements made, it was stated on the Twitter account that the coins named Monero (XMR), Zcash (ZEC) and Dash (DASH) will be removed from Bittrex as of January 15, 2021. According to CoinMarketCap data, in the last 24 hours, Monero lost 16.51 percent to $ 135.13, Zcash lost 10.91 percent to $ 58.16, and Dash 12.47 percent to $ 88.96 (Reynolds, 2021).

In the past, several other exchanges had also removed privacy-focused cryptocurrencies from their lists. For example, OKEx Korea and Upbit had stopped trading cryptocurrencies for similar reasons.

Figure 3.2 Source: https://twitter.com/bittrexexchange/status/1345056010981892096?s=

References

Aaron, S. (2020, November 17). *The Complete Guide to Monero Cryptocurrency*. Bitdegree. https://www.bitdegree.org/crypto/monero#the-history-of-monero

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, 5 18). Zerocash: Decentralized Anonymous Payments from Bitcoin https://whitepaper.io/document/13/zcash-whitepaper

Binance Coin price today, BNB marketcap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/binance-coin/

Binance Academy. (n.d). *What Are Nodes?* Retrieved December 31, 2020, from https://academy.binance.com/en/articles/what-are-nodes

Binance (2020, January 27). *Bitcoin Halving 2020: Some FAQs on What It Is and Why It Excites People.* https://www.binance.com/en/amp/blog/421499824684900376/Bitcoin-Halving-2020-Some-FAQs-on-What-It-Is-and-Why-It-Excites-People

Binance Academy. (n.d.) *The Bitcoin Halving*. Retrieved December 31, 2020, from https://academy.binance.com/en/articles/what-is-bitcoin#chapter-4-the-bitcoin-halving

Blockwolf. (n.d.). *Zcash (ZEC)*. Blockwolf. https://blockwolf.com/zcash/

Bitcoin Cash price today, Bitcoin Cash market cap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/bitcoin-cash/

Bitcoin price today, Bitcoin market cap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/bitcoin/

Bitcoin SV price today, Bitcoin SV marketcap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/bitcoin-sv/

Bitcoin Treasures. (n.d.). *Bitcoin Treasuries* Retrieved December 31, 2020, from https://bitcointreasuries.org

BitInfoCharts (n.d.). *Bitcoin Cash (BCH) price stats and information.* .https://bitinfocharts.com/bitcoin%20cash/

BNB nedir? | Binance Academy. (n.d.). Retrieved January 03, 2021, from https://www.google.com.tr/amp/s/academy.binance.com/tr/articles/what-is-bnb.amp

Ceicdata (n.d.). *European Union Money Supply M2.* Retrieved December 31, 2020, from *https://www.ceicdata.com/en/indicator/european-union/money-supply-m2*

Coin Market Cap. (n.d.). *Bitcoin Cash*. Coin Market Cap. https://coinmarketcap.com/currencies/bitcoin-cash/

Coinmarketcap. (n.d.). *About Bitcoin*. Retrieved December 31, 2020, from https://coinmarketcap.com/currencies/bitcoin

Coindesk. (2020, October 20). Monero's Spagni: *Cryptographers Are Always Going to Be One Step Ahead of Regulators.* Youtube. https://www.youtube.com/watch?v=5QQOhd3nckM

Companies (n.d.) *Largest Companies by Market Cap*. Companies Market Cap. Retrieved December 31, 2020, from https://companiesmarketcap.com/

Dash price today, DASH market cap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/dash/

D, E. (2021, 01 02). *Bittrex'den Delist Edilen Popüler Altcoin Projesine, Büyük Destek Geldi.* beincrypto. https://beincrypto.com.tr/bittrexden-delist-edilen-populer-altcoin-projesine-buyuk-destek-geldi/

Digiconomist. (n.d.). *Bitcoin Energy Consumption Index.* Retrieved December 31, 2020, from https://digiconomist.net/bitcoin-energy-consumption/

Ethereum price today, Ethereum market cap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/ethereum/

Frankenfield, J. (2020, 01 27). *Ethereum*. Investopedia. https://www.investopedia.com/terms/e/ethereum.asp

Frankenfield, J. (2020, December 10). Bitcoin Cash. Retrieved January 03, 2021, from https://www.investopedia.com/terms/b/bitcoin-cash.asp

Frankenfield, J. (2020, December 10). *Bitcoin Cash Definition*. Investopedia. https://www.investopedia.com/terms/b/bitcoin-cash.asp

Franceschi-Bicchierai L. (2020, September 11). *The IRS Wants to Buy Tools to Trace Privacy-Focused Cryptocurrency Monero.* Vice. https://www.vice.com/en/article/wxq9xx/the-irs-wants-to-buy-tools-to-trace-privacy-focused-cryptocurrency-monero

Getmonero (n.d.). *About Monero*. Retrieved December 31, 2020, from https://www.getmonero.org/resources/about/

Getmonero (n.d.). *Ring Signatures*. Retrieved December 31, 2020, from https://www.getmonero.org/resources/moneropedia/ringsignatures.html

Getmonero (n.d.). *Stealth Adresses.* Retrieved December 31, 2020, from https://www.getmonero.org/resources/moneropedia/stealthaddress.html

Getmonero (n.d.). *RingCT*. Retrieved December 31, 2020, from https://www.getmonero.org/resources/moneropedia/ringCT.html

Getmonero (n.d.). *RandomX*. Retrieved December 31, 2020, from https://www.getmonero.org/resources/moneropedia/randomx.html

Getmonero (n.d.). *Mining*. Retrieved December 31, 2020, from https://www.getmonero.org/resources/moneropedia/mining.html

Getmonero (n.d.). *Smart Mining. Retrieved December 31, 2020, from* https://www.getmonero.org/resources/moneropedia/smartmining.html

GitHub. (n.d.) *Bitcoin*. Retrieved December 31, 2020, from https://github.com/bitcoin/bitcoin

GitLab. (2019, December 31). *Kovri*. Retrieved December 31, 2020, from https://gitlab.com/kovri-project/kovri/

Github. (n.d.). *monero-project.* Retrieved December 31, 2020, from https://github.com/monero-project/monero

Harper, C. (2020, December 31). *Ripple to Meet With SEC in First Pretrial Conference on Feb. 22.* Retrieved January 03, 2021, from https://www.coindesk.com/ripple-to-meet-with-sec-in-first-pretrial-conference-on-feb-22

Kenton, W. (2020, December 07). *What Is Ether cryptocurrency?*. Retrieved January 03, 2021, from https://www.investopedia.com/terms/e/ether-cryptocurrency.asp

Learning Resources. (2020, July 25). Retrieved January 03, 2021, from https://www.dash.org/learning-resources/

Maddrey, D. [@natemaddrey]. (2020, December 22). *Over the course of 2020 BTC added over $300B to its market cap. The amount of daily active addresses doubled, and the number of addresses holding at least 0.01 BTC grew by over 700k.* [Tweet]. Twitter. (https://twitter.com/natemaddrey/status/1341457544364105729).

Mining. (2020, July 09). Retrieved January 03, 2021, from https://www.dash.org/mining/

Monero price today, Monero marketcap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/monero/

Nakatomo S. (2008, October 31). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Bitcoin. https://bitcoin.org/bitcoin.pdf

PayPal. (2020, November 24) *PayPal Consumer Fees.* https://www.paypal.com/us/webapps/mpp/paypal-fees

Peters, K. (2020, 09 23). *zk-SNARK*. Investopedia. https://www.investopedia.com/terms/z/zksnark.asp

Reiff, N. (2019, June 25). *A History of Bitcoin Hard Forks.* Investopedia. https://www.investopedia.com/tech/history-bitcoin-hard-forks/

Reynolds, K. (2021, January 01). Bittrex to Delist 'Privacy Coins' Monero, Dash and Zcash. Retrieved January 03, 2021, from https://www.coindesk.com/bittrex-to-delist-privacy-coins-monero-dash-and-zcash

XRP price today, XRP. market cap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/xrp/

Sharma, R. (2018, 03 26). *Edward Snowden Comes Out in Favor of Zcash*. Investopedia. https://www.investopedia.com/news/edward-snowden-comes-out-favor-zcash/

Sharma, R. (2018, 05 14). *What Is Zcash?* Investopedia. https://www.investopedia.com/tech/what-zcash/

Syracuse, D. Boehm, J. & Lundgren, N. (2020, September 9) *Anti-Money Laundering Regulation of Privacy-Enabling Cryptocurrencies*. Perkinscoie. https://www.perkinscoie.com/en/news-insights/anti-money-laundering-regulation-of-privacy-enabling-cryptocurrencies.html

Tiwari, A. (2020, December 10). 5 Amazing Benefits of Ripple/XRP Crypto. Retrieved January 03, 2021, from https://btcmanager.com/5-amazing-benefits-of-ripple-xrp-crypto/

US Department of The Treasury. (2020, December 18). *The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions*. Retrieved December 31, 2020, from https://home.treasury.gov/news/press-releases/sm1216

Wheal, C. (2019, August 25). History of the DASH cryptocurrency. Retrieved January 03, 2021, from https://dex.openledger.io/history-of-the-dash-cryptocurrency/

XRP (XRP) Fiyatı, Grafikler, Piyasa Değeri. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/tr/currencies/xrp/

XRP. (2020, October 22). Retrieved January 02, 2021, from https://ripple.com/xrp/

Zcash price today, Zcash marketcap, chart, and info. (n.d.). Retrieved January 03, 2021, from https://coinmarketcap.com/currencies/zcash/