POLITECNICO DI TORINO

Corso di Laurea in Engineering and Management

Tesi di Laurea Magistrale

CRYPTOCURRENCY: ARE WE READY TO DEMONETIZE THE WORLD?

POLITECNICO
DI TORINO

Dipartimento
di Ingegneria Gestionale
e della Produzione

Relatore:
prof.ssa Elisa Ughetto

Candidata:
Aydan Hasanli

OCTOBER 2021

Abstract

With the advancement of technology and the proliferation of the use of the Internet, commerce that has been forced to change has led to a change in the form of money and has added new concepts and applications to our lives. The digital economic formation has arisen as a result of the entry of the world into the digitalization process and its reflection in the economy. Money gradually began to lose its physical existence and paved the way for the creation of a society that does not use cash through digitization. The last link in this evolution is cryptocurrencies with Blockchain technology.

Cryptocurrencies can play an important role in the global economy due to their high transaction speed and low transaction costs. This study assesses the potential of cryptocurrencies as reserve money, the opportunities it offers and the challenges it faces. This study also discusses what the possible prospects for central banks will be if crypto money creates an alternative currency to existing currencies.

CRYPTOCURRENCY: ARE WE READY TO DEMONETIZE THE WORLD?

Table of Contents

INTRODUCTION

The fact that people who lived as nomads in ancient historical eras did not need a commodity that they would accept as money changed with the transition to a sedentary life. Due to the differentiation of needs, the barter method used at that time was insufficient. In addition, the first examples of money in history appear as commodities. In ancient times, many objects were accepted as means of exchange, such as gold, silver, copper, salt, seashells, large stones, and pepper. In this context, the object used as a means of change in parallel with the increase in people's knowledge was constantly changing. First, precious metals were used, then paper, and now it is about to lose its physical existence. The reason this study emerged is because cryptocurrencies can cause radical changes in the existing financial system. The end point of the evolution of money is digital currencies. Blockchain, a special type of distributed ledger technology, was introduced in 2008 in an article by Satoshi Nakamoto, and Bitcoin, a blockchain product, was launched in 2009. This system, which is different in many aspects, can demonstrate creative destruction, as Schumpeter said. The hypothesis of the study is that cryptocurrencies can be used as money, and it is possible that all payments can be made with virtual money in the future. Although not yet used heavily enough, it is possible that it will become a global change tool with the features it offers. It can have a say in global trade thanks to its decentralized structure, low transaction fees, high transaction speed, independence from authorities, and elimination of the need for intermediaries. In traditional monetary systems, trust was the most important underlying element. Discussions have arisen about whether the traditional monetary system, whose credibility has been eroded for economic and political reasons, can be regulated. In the course of these discussions, cryptocurrencies emerged and consideration began on whether there would be a system that could replace the money used in the traditional monetary system. It is believed that it is important to the economy how central banks, which have the power to print money and conduct monetary policy, will respond to the use of cryptocurrencies. In this case, the question of how central banks will regulate their policies is one of the most important issues to be explored. The aim of this study is to find out if cryptocurrencies will replace fiat currencies and to find out how crypto central banks are currently taking cryptocurrencies.

The purpose of the study is to better understand cryptocurrencies, understand their impact on reserve management, and determine the functions that cryptocurrencies should receive in the

development process. Obviously, cryptocurrencies can affect financial markets. However, it has not yet reached a size that could affect monetary and fiscal policy. Regardless, countries are keen to turn this technology into an opportunity with appropriate research, rather than being indifferent. Another goal of the study, which evaluates cryptocurrencies from a different perspective, is to shed light on those who will conduct a comprehensive study on the subject.

1. WHAT IS CRYPTOCURRENCY AND HOW DOES IT WORK? DISTINCTIVE FEATURES

Cryptocurrencies are digital assets intended to be used as a tool for exchange and measurement of value. They ensure the security of transactions through the use of cryptographic algorithms. They have no owners or managers. These systems, made up of publicly available codes, are the sole owner of these systems. All questions, such as how money will be distributed among these users, how and under what conditions new coins will be released to the market, and how transactions will take place topologically, are structured in source codes, and this code can be viewed by anyone at any time, but cannot be changed by anyone. However, every transaction made using these currencies is recorded in a shared ledger for each user. Thanks to the cryptographic algorithms used by the blockchain system, it is impossible to change anything on any user's laptop at any time. The reason it gets more attention than other currencies in the world is because it is organic. In other words, crypto coins are not controlled or managed by the government or center.[1] Cryptocurrency is a virtual currency system, similar to a standard currency, that is used as a means of payment when purchasing goods and services, without being connected to a reliable central system. Cryptocurrencies depend on the transmission of digital data and by using cryptographic (encryption) methods they ensure that they are legal and unique.[2]

Crypto coins are intangible coins. They can be converted to physical currency. Although Bitcoin is the most famous, there are over a thousand varieties such as Ethereum, Litecoin, Ripple. Crypto coins are decentralized, not subordinate to a specific institution or organization, and are not included in the structure that determines their value. This is driven by the encryption community. They do not apply all over the world, and some legal regulations are also accepted.[3]

Cryptocurrency is a blockchain-based system that only exists on the web. The blockchain system is discussed in details from technological aspect in the third part of thesis work. The amount of each individual account and transactions carried out on that account are recorded in the database. In this sense, the system is the same as the banking system. The money is sent to another account with an account number consisting of the numbers associated with the sender's account. There are

[1] Franco, P. (2015). Understanding Bitcoin. UK: John Wiley and Sons Ltd

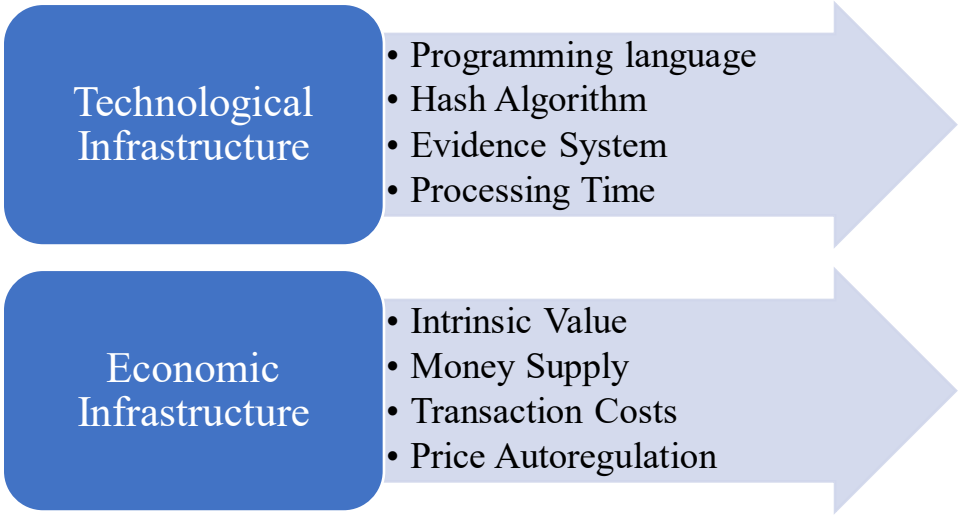
[2] Harwick, C. (2016). Cryptocurrency and the Problem of Intermediation. http://www.independent.org/pdf/tir/tir_20_04_05_harwick.pdf

[3] Gandal, N. and Halaburda, H. (2014). Competition in the Cryptocurrency Market. https://www.econstor.eu/bitstream/10419/103022/1/791932281.pdf

no physical changes. This is nothing more than information stored in the database, only numbers are transferred from one place to another. All cryptocurrencies work in the same way. When using cryptocurrency, there must be public and private keys that appear as random strings of numbers and letters. Private keys should not be shared with anyone, the private key should be kept in a written and secure place. It is not recommended to store in easily accessible places. If your private key is lost, all authorization controlled by that key will be lost. In cryptocurrencies, a transaction is not approved by a central authority, but by a peer-to-peer computer network, and consensus is reached on the transaction. This has been shown to be one of the most attractive and disruptive aspects of cryptocurrencies. The future is believed to be in this direction with the transformation of types of cryptocurrency money into a structure controlled by people rather than a central authority such as banks. The growth and spread of the day by day makes it possible for the cryptocurrency coins to be recognized, which are used to buy goods and services. Bitcoin is the most famous of all cryptocurrencies at the moment. Companies are trying to discover bitcoin and other cryptocurrencies. However, Bitcoin's destructive advantage does not seem to be easy to overcome. Many of the world's leading companies accept payments in cryptocurrency, and the number of these companies is growing day by day. Very serious companies like Playstation accept cryptocurrency payments.

The basic idea underlying the logic of crypto currencies is that there is no central and singular record keeping system. Instead, millions of copies of this registry are distributed in the hands of each user, and millions of users are writing the ledger at the same time, witnessing each transaction. This means that each copy in the hand of each owner of the ledger is filled in simultaneously. A malfunction in a user's notebook as a result of an error or malicious intent is corrected by looking at the records in the majority of the system, and consistency is ensured within milliseconds. Crypto currencies consist of 2 basic components: technological infrastructure and economic structure.

Figure 1: Infrastructure of Cryptocurrencies[4]



Programming language - Blockchain projects using C++ include: EOS — C++ is the main programming language of EOS preferred for its flexibility to run extensive applications on top of the blockchain. EOS also supports any language that compiles into WebAssembly (WASM)

Hash algorithm - The hash function is an algorithm or subroutine that maps variable length data sets to fixed length data sets. The values returned from hash functions are called hash values, hash codes, hash sums, checksums, or simply hashes. Hash functions are used in the database to quickly find a data searched in the table or to speed up data comparison processes, to detect the same or similar records in a large file, to find similar sequences in the DNA sequence, etc.

Evidence system - Proof-of-work method is used if it is manipulated by miners or if 2 different results come from 2 different miners. It must verify whether the transaction in question is correct or not. After the processor consumption, which will have proof of work, is realized, the block is not changed unless the same work is done. This does not seem possible at the moment. Since each block in the chain depends on its own priorities, making a block change means recalculating the next ones.

Processing Time - On the Bitcoin network, the average confirmation time for a BTC payment is about 10 minutes. However, transaction times can vary wildly.

[4] Seetharaman, A., Saravanan, A., Patwa, N., and Mehta, J. (2017). Impact of Bitcoin as a World Currency. Accounting and Finance Research, 6(2), 230.

So talking about bitcoin, it is a cryptocurrency using the SHA-256 cryptography algorithm, written in C ++ language and encoded based on the Proof of Work algorithm. These features are variables that define the technological infrastructure of Bitcoin. The technological infrastructure determines the issues such as the duration of the transactions made using this currency and the security of the transactions. Questions such as how much new Bitcoins will be released to the market in how long, how they will be distributed and transaction costs are related to the algorithm created for the economic infrastructure. For example, in Bitcoin, the reward miners received for a block they mined decreased from 50 BTC in 2009 to 25 BTC in 2012 and 12.5 BTC in 2016. On the other hand, the total mining power (Hash Rate) increased exponentially. As a tertiary variable, the digging power required to excavate 1 block also increases exponentially. Therefore, the total supply will continue to increase at a decreasing rate as the number of people using the currency increases. These regulations on the money supply are carried out by the algorithm of the cryptocurrency.[5]

The users of the system provide mediation services through their own electronic devices (computer, telephone, etc.) in the process of performing each other's transfer transactions. In return for this brokerage service, the system sends the newly produced cryptocurrencies as an intermediary fee to the account of the owner of the electronic device. In this way, the money supply to the system is realized. As more people start to use cryptocurrency, the transfer transactions increase in the system and therefore the money supply increases through the transaction fees charged by intermediaries. In this way, the transaction costs in the system turn into a money supply mechanism that does not burden the user and distributes the money in direct proportion to the labor given to the system.

We can define cryptocurrencies in a single sentence as a registry that is not managed by any center and records cannot be changed retrospectively. Although it sounds commonplace, the fiat currencies used in today's monetary system are essentially no different from this. The money in bank accounts consists of a digital register kept on the main computers of the bank. In this case, it can be concluded that the confidence in fiat currencies in today's monetary system stems from the confidence that this registry will not be changed improperly. Confidence that these registers cannot be tampered with is also equal to the multiplication of trust in the bank where the records

[5] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. New Jersey: Princeton University Press.

are kept, in the supervisory bodies that oversee the bank, and in government agencies that regulate supervisory agencies. If confidence in any component of the system is zero, the entire system may lose its functionality. Terminologically speaking, fiat currencies have no intrinsic value. They derive their value from the confidence that they will be used as a medium of exchange for the goods and services they correspond to in the economy they depend on. Today, central banks that supply fiat currencies do not supply them based on a particular precious metal or asset. There are conflicting opinions in the literature regarding whether financial instruments mentioned as cryptocurrencies should be classified as currency or assets. To ensure terminological consistency with the literature, these instruments will continue to be referred to as cryptocurrencies for the remainder of the study.

In multilateral agreements, in order to solve the problem of insecurity between the parties, the possibility of failure of the parties to fulfill their obligations, there has been a need for intermediaries throughout the history of humanity. Today, intermediaries operate in many areas from simple general purpose loan purchases to letter of credit transactions in international trade. However, many studies in the literature question the contribution of the presence of intermediaries to market efficiency.[6]

Predictions about the future of cryptocurrencies are quite different from each other. The main reason for this difference is the differences in the prediction process of the situations that are supposed to be encountered in the evolution of crypto money. Many experts think that only one or a few of the thousands of cryptocurrencies today can survive in the long term. The basis of this view is the volatility created by the new cryptocurrency public offerings (ICO), which do not have a concrete function or technological superiority. It is expected that the effects of cryptocurrencies on the global financial and economic system will occur through various channels. Some advantages of the system, which provides many advantages in a constructive and unifying nature for both individual and corporate users, may appear as disadvantages in certain situations.[7]

The most outstanding feature of crypto currencies that can be considered as revolutionary is that they have a decentralized recording structure. This structure, on the one hand, makes

[6] Ahn, J., Khandelwal, A. K., and Wei, S.-J. (2011). The role of intermediaries in facilitating trade. Journal of International Economics, 84(1), 73-85.

[7] Burkart, M., and Ellingsen, T. (2004). In-kind finance: A theory of trade credit. American Economic Review, 94(3), 569-590.

cryptocurrencies the strongest candidate to become the global reserve currency, on the other hand, it has the potential to make the extremely profitable brokerage market more competitive in the medium term and to eliminate financial intermediation in the long term. When the same independent structure is examined from a micro perspective, it offers systems with mathematically impossible levels of payment security to be broken even with quantum computers and can also ensure the security of personal information.

An initial coin offering (ICO) is the cryptocurrency industry's equivalent to an initial public offering (IPO). A company looking to raise money to create a new coin, app, or service launches an ICO as a way to raise funds. Interested investors can buy into the offering and receive a new cryptocurrency token issued by the company. This token may have some utility in using the product or service the company is offering, or it may just represent a stake in the company or project. Despite increasing market volatility and making the market vulnerable to Pump & Dump operations, they are an indispensable part of the evolutionary process of cryptocurrencies. The opinions arguing that cryptocurrencies will be accepted collectively on the basis of states or by the masses in the future suggest alternative cryptocurrency supply approaches to ICOs in the medium term.[8] An initial coin offering (ICO) is the cryptocurrency industry's equivalent to an initial public offering (IPO). A company looking to raise money to create a new coin, app, or service launches an ICO as a way to raise funds. Interested investors can buy into the offering and receive a new cryptocurrency token issued by the company.

One of the biggest factors that will allow cryptocurrencies to be accepted is accessibility. Cryptocurrencies, which can be used by every individual with internet access in the world, allow financial transactions to be carried out instantly and without an intermediary in any digital environment, from smart mobile phones to personal computers. The only requirement to join this system is an internet connection. When we look at fiat money, it is possible to talk about an electronic money system in which every human being is born in today's society. Although fiat currencies offer similar convenience in daily transactions in terms of accessibility, they fall far behind the potential of cryptocurrencies in international money transfers in terms of both time and cost. In international monetary transfers, cryptocurrencies stand out significantly in terms of accessibility in such areas, since processes such as exchanging exchange rates with a certain

[8] Seetharaman, A., Saravanan, A., Patwa, N., and Mehta, J. (2017). Impact of Bitcoin as a World Currency. Accounting and Finance Research, 6(2), 230.

currency on a cross currency and obtaining approval from regulatory authorities are not available in crypto currencies. In addition, new features such as the ability of transfer transactions within milliseconds and 24/7 transactions, which are highlighted by new generation crypto currencies, are among the financial innovations of crypto currencies.

The decentralized nature of cryptocurrencies is a feature with the potential for disruptive productivity. This feature is not only limited to eliminating the rule of regulators or reducing the market share of intermediaries. The fact that a currency is not decentralized means that it cannot be exploited to maximize the interests of a single person or group. These qualities provide cryptocurrencies with the capacity to be a cross-border value storage unit and transfer tool, making cryptocurrencies a strong candidate for use as an international reserve currency. Cryptocurrencies have different approaches to protect personal information. Many currencies, including Bitcoin, use an identity management system called an anonymous pseudonym. In this system, accounts can be followed by anyone and are transparent. On the other hand, it is technically not possible to obtain information about which nickname in the system belongs to which real or legal person without the cooperation of crypto money exchanges. Therefore, this system does not provide the protection of personal information completely and leaves the system semi-transparent. However, cryptocurrencies like Monero use an untraceable personal data protection system called anonymous. In this system, the parties are not visible to each other, including their nicknames. This system allows the protection of personal information completely. The disadvantage is that it makes it impossible to track cryptocurrencies, making them widespread for financing terrorism, drug trafficking and similar illegal activities.

In recent years, many hacking cases related to crypto currencies have come to the fore. There is a very important detail to take into account in these cases ranging from the stealing of the wallets of individuals to the evacuation of the accounts of huge brokerage houses. Not a single one of these “hacking” cases occurred as a result of breaking the blockchain system that forms the basis of the cryptocurrency. The encryption algorithms used by many cryptocurrencies use mathematically improbable encryption methods such as SHA 256. All cases are attacks that have occurred as a result of individual errors of users or vulnerabilities in the codes of the brokerage houses on their main computers. On the other hand, according to the security analysis study published by Vovchenko in 2017, there is no significant difference between the frequency of security problems encountered in internet banking and the frequency of security problems

encountered during the use of crypto money, and almost all of the security vulnerabilities occur due to user errors.[9]

Mining, which is a concept that cryptocurrencies have recently brought to the financial literature, is one of the points where the blockchain system is subject to the most criticism. The energy used by computers in encryption and password guessing processes is quite high in first generation cryptocurrencies and it is not possible for first generation systems to work without this mining activity. The costs of electricity and worn out equipment consumed during this process create a new burden on limited world resources. At the beginning of 2018, the amount of electricity spent for crypto money mining reached a point where it would exceed the annual electricity consumption of some developed countries. Realizing this problem, new cryptocurrency programming teams have developed systems that will be able to work without the need for a mining system. One of the first examples of this is the cryptocurrency-like electronic asset Ripple, which is considered to have a central operating system. As will be discussed in detail in the following sections, at the design stage of the third generation cryptocurrencies, algorithms that eliminate the mining system structurally were developed and the decentralized structure of the system was maintained.

2. THE EMERGENCE OF CRYPTOCURRENCY

The fact that the blockchain system contains relatively hard to understand concepts and the system has not yet been accepted worldwide are among the factors that put pressure on the potential of use of cryptocurrencies. In addition to these factors, a large number of speculators entering the cryptocurrency markets in hopes of high returns and exiting the market in panic moments significantly increase the volatility of the markets. This volatile investment environment adversely affects the adaptation process. Investors entering the system without mastering the technological infrastructure and economic models of blockchain and crypto currencies should understand the algorithm and anticipate future market dynamics, rather than making investment decisions according to the usual capital market behaviors.

[9] Vovchenko, G., Tishchenko, N., Epifanova, V., and Gontmacher, B. (2017). Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them. European Research Studies Journal, 20(1), 36-48.

The first crypto currency Bitcoin remained as the only crypto currency from 2009, when it was launched to the market, until 2011. During this time, cryptocurrencies, which were a very new idea, started to be accepted and used by the increasing masses. The relatively widespread use of the protocol brought with it debates on scale issues. Many software experts in the cryptocurrency field have proposed new blockchain systems to make the blockchain protocol capable of serving larger audiences without any problems. The main factor that determines which system will be accepted has been the decisions of the investors.

Investors participating in this highly uncertain market can be categorized as speculators or users according to their behavior in the market. A large number of speculators, whose main purpose is individual value maximization and who do not need to have knowledge about the usage areas or technological features of cryptocurrencies, operate in the crypto money markets. The group defined as users consists of communities such as early adopters of technology and software developers. The group of users consists of individuals who mostly have a command of the economic and technological infrastructure of the systems and even use these systems in their daily financial transactions. The group of users who invest only with the motivation that currencies that are developed in terms of economic and technological models will remain in the market in the long term, like a fan base, they hold certain crypto coins even if they are damaged. This group is also referred to as the Hodl Gang (Retention Gang) on the internet. In the period between 2008 and 2012, the dominance of the mass of users, which is thought to constitute almost the entire market, over the markets ended with speculators entering the market with huge amounts of money and taking over the majority of the market. With speculators taking over the majority of the market, it becomes difficult for cryptocurrencies with useful uses and capacity to create value to attract investors' attention.[10]

The changes to be made regarding the blockchain protocol could not be implemented mostly due to the differences of opinion between the users in the system. The proposed changes to the protocol could not be realized due to both technical and political constraints. Since any protocol change proposal that will solve the scale problem of Bitcoin will increase the supply of crypto money, users with BTC (Bitcoin) predicted that they will face a loss of value, so the protocol changes that will increase the BTC supply did not lean. The main technical problem preventing

[10] Corbet, S., Larkin, C. J., Lucey, B. M., and Yarovaya, L. (2018). Kodakcoin: A Blockchain Revolution or Exploiting a Potential Cryptocurrency Bubble?

protocol change is the occurrence of separations called fork. Although these separations are named differently according to the way they occur, in principle, they refer to situations where all users do not accept the new protocol rules when the protocol of a cryptocurrency is changed. The new protocol and the old protocol are now technically two different currencies. One of the most recent examples of these types of separation, called Hard Fork as a technical term, is Bitcoin Cash. Since the Bitcoin Cash protocol, which increases the transaction speed by updating the code that limits the block size to 1MB in the Bitcoin protocol to 8 MB, is not accepted by all users, there are two different cryptocurrencies named Bitcoin and Bitcoin Cash today.[11]

Hard Forks are not the only way for new cryptocurrencies to emerge. Since crypto currencies are open source with a few exceptions due to their nature, it is possible to introduce new crypto currencies by making small changes on the code that makes up the protocol. One of the first inspirations of bitcoin called Spin-Off is Litecoin (LTC), which entered the market in 2011. Today, LTC, which is still among the top 10 cryptocurrencies in terms of market volume, has changed the SHA256 consensus algorithm used by Bitcoin with a different algorithm called Scrypt, and has increased the maximum coin amount 4 times. While these changes, which reduce the block solving time from 10 minutes to 2.5 minutes, partially solved the scale problem, the protocol used is the same logically.

The Initial Coin Offering (ICO) concept is the most common method of the emergence of new cryptocurrencies today. This method, which can be used by cryptocurrencies with both inspiration and source code created from scratch, offers a certain amount of cryptocurrency to investors through various methods similar to stock public offering. Currencies that have had high returns since the IPO popularized this method. For example, NXT[12] increased by 1.500.000% from

[11] Nian, L. M., and Chuen, D. L. K. (2015). Introduction to Bitcoin. Handbook Of Digital Currency. Elsevier Inc..

[12] Nxt is an open source blockchain platform and the first to rely entirely on a proof-of-stake consensus protocol. Launched in November 2013 and written from scratch in Java, Nxt is proof that blockchain technology is not only about simple transfer of value but also has the potential to revolutionize many aspects of our lives with the various decentralized applications that can be built with it. Today, Nxt remains one of the most tested and reliable platforms in the industry, influencing numerous other projects. With its many easy to use modular built-in features, Nxt covers most of the dApp use cases and at the same time is perfectly suitable for private blockchain implementations.

its public offering in 2013 until the end of 2017. A more recent example, IOTA[13], which went public in 2017, rose by over 300,000% by the end of the same year. On the other hand, some of the cryptocurrencies invested in the public offering phase in anticipation of high profits are malicious public offerings derived from inspirational codes that have no originality. However, many cryptocurrencies with the possibility of being one of the future crypto currencies have also been opened to the market with this method.[14]

ICOs do not always promise to offer a new currency, payment method, or exchange tool to be used as a value storage system. Although such public offerings are categorized as crypto money, their main purpose is to fund specific projects or companies. While the company transparently holds a certain percentage of these cryptocurrencies, which are used as stocks or donations, it seeks to raise capital by offering some of it to the public. This method, which has been widely used as an alternative to global crowdfunding companies, has started to be used by companies that are described as start-ups today.

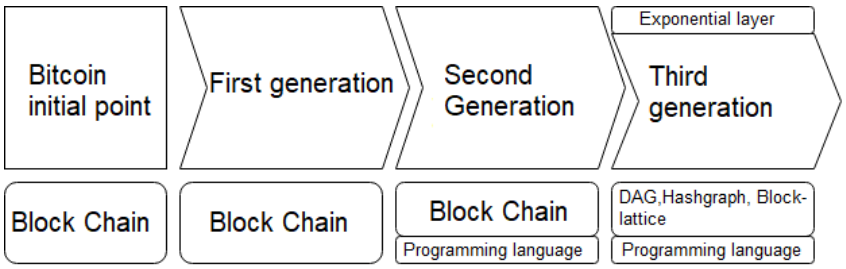
During the emergence of new crypto currencies, there have been periods of significant technological leaps. As of the date of this study, 1523 different cryptocurrencies on the market are traded on 8715 different exchanges spread around the world. The cryptocurrency market has a market capitalization of at most over 813 billion USD, and its daily trading volume has exceeded 70 billion USD. In the process of launching each new cryptocurrency, a new economic idea is put forward or a technological development is proposed. It is possible to classify these cryptocurrencies under 3 generations according to their emergence ideas and technological structures.[15]

[13] IOTA is an open-source distributed ledger and cryptocurrency designed for the Internet of things (IoT).[1] It uses a directed acyclic graph to store transactions on its ledger, motivated by a potentially higher scalability over blockchain based distributed ledgers.[1] IOTA does not use miners to validate transactions, instead, users that issue a new transaction must approve two previous transactions and perform a small amount of proof of work.[2] Transactions can therefore be issued without fees, facilitating microtransactions.

[14]Chohan, U. (2017). Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability

[15]Tasca, P. (2015). Digital Currencies: Principles, Trends, Opportunities, and Risks. https://faculty.fuqua.duke.edu/~charvey/Teaching/898_2017/Readings/Tasca.pdf

Figure 2. Three Generations of Crypto Coins[16]



As discussed before, the starting point of all crypto currencies is Bitcoin. Bitcoin remained the only cryptocurrency for two years since 2009, during which time those who adopted the blockchain system had the opportunity to discuss the blockchain structure on the internet and on various platforms. One of the most striking features as the negative aspects of Bitcoin was the scale problem. Considered by the community as the currency of the future, Bitcoin was too slow to use in daily transactions, and this speed was slower as the number of users increased. Despite the system having 7 to 4 transactions per second, payment methods such as Visa and Mastercard of the traditional financial system had the capacity to process more than 4000 transactions per second. Another notable problem was the structure of the mining system. The fact that miners, who play a critical role in the operation of the system, caused energy consumption to compete with countries around the world, as well as increased demand for computer processors and graphics cards, negatively affecting the market. The main problem that arises in mining-based blockchain systems is that 51% of the miners are likely to come together and take control of the chain. The existence of mining pools is one of the biggest factors that increase this risk. In 2014, the ghast.io pool came close to diverting more than 50% of the total mining power alone and was temporarily prevented by the dispersal of miners to other pools.[17]

First generation cryptocurrencies aimed to find solutions to the structural problems of Bitcoin and changes in the blockchain infrastructure. In addition, using the distributed ledger system of the blockchain, currencies containing alternative solutions for today's information

[16] Darlington III, J. K. (2014). The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency Through Benefit Analysis.
[17] Darlington III, J. K. (2014). The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency Through Benefit Analysis.

market have been revealed. First generation cryptocurrencies have concentrated on alternatives methods in terms of Hash algorithm and block size. The SHA 256 algorithm and the increasing difficulty of solving blocks increase mining costs day by day in terms of both energy costs and hardware investments. In 2011, Charlie Lee launched the crypto currency Litecoin, which he created using the Scrypt Hash algorithm, which he predicted would reduce energy and hardware costs associated with mining. The change of the hash algorithm in this direction has allowed many computers that can be classified as gaming computers to dig this crypto currency by using the processors of their video cards. Litecoin is still among the top 10 cryptocurrencies with the highest market value today. Among the first generation cryptocurrencies, there are also cryptocurrencies such as Namecoin, which aims to benefit from blockchain technology not only financially but also technologically. In this blockchain structure, which presents an infrastructure that aims to replace DNS servers, the crypto currency is not only a currency, but also a tool with a technological function.[18]

The crypto currencies that we classify as the second generation are crypto currencies that redesign the blockchain system by making it programmable. Programmable blockchain enables the creation of smart contracts and enables them to be secure contract tools that can be used not only as a currency or financial instrument, but in any field. The first and most famous example in this regard is Ethereum. Although the working logic of these systems, which are described as a distributed computing platform as well as being a blockchain-based crypto currency, is based on the blockchain infrastructure, the way they are implemented is highly developed. There are instances where Ethereum is currently being used as a substitute for futures contracts and options around the world. On the other hand, it was not possible for 2nd generation cryptocurrencies to eliminate problems such as mining and scaling due to the fact that they were implemented based on the topological structure of the blockchain system.[19]

The biggest difference that distinguishes 3rd generation cryptocurrencies from others is that they are designed to be programmable in multiple layers. The multi-layered realization of transactions is considered a big development that will create a new generation. This is because multi-tier platforms allow multiple cryptocurrencies to work together. In addition, it provides the

[18] Heid, A. (2013). Analysis of the Cryptocurrency Marketplace. Retrieved February, 15

[19] Chen, C. Y., Härdle, W. K., Hou, A. J., and Wang, W. (2018). Pricing Cryptocurrency options: the case of CRIX and Bitcoin.

opportunity to solve the scaling problem without creating any security weakness. When we define it in this way, Cardano can be considered as a 3rd generation crypto currency. Considering that 3rd Generation cryptocurrencies are designed to be a component of a multi-layered crypto financial system, it is possible to classify the IOTA cryptocurrency as 3rd Generation. IOTA, which is completely different in the Tangle algorithm blockchain system it uses, theoretically enables countless transactions per second. It is possible that multi-layered cryptocurrency systems can eliminate the function of intermediary institutions that trade between cryptocurrency and fiat money. The existence of these intermediaries, called crypto exchanges, affects their functionality negatively because they conflict with the basic principles of crypto currencies.

Crypto currencies have been traded on intermediary crypto exchanges in exchange for fiat currencies since 2009, when they were launched on the market. These brokerage houses have turned into disadvantages or eliminated many advantages offered to the users of crypto currencies. Although it is impossible to break the blockchain system, the accounts of brokerage houses are susceptible to breakage. The ability of cryptocurrencies to significantly reduce or even eliminate transaction costs has lost its meaning with the transaction fees collected by these intermediary institutions, the shape of the institutions that receive the commission has changed and transaction costs have preserved their existence. Transaction fees not paid to banks have started to be taken by these intermediary institutions. Crypto exchanges also weaken the decentralization of crypto currencies from two different points. These points are collective mining exchanges and fiat exchanges. In mining exchanges, the Hash Power of miners is designed to increase as they come together and dig. Therefore, when miners excavate collectively in these pools rather than digging alone, their earnings per individual are higher. Thus, the main motivation for gathering miners in pools is the maximization of mining earnings per individual.[20]

While the blockchain infrastructure is creating the transaction book, it is a big risk for the system that the majority of the system is in the hands of a single person, since it is programmed to accept the inputs in the majority of the system. This threat is named as a 50 percent attack. Today, more than seventy-seven percent of the total mining hash power is provided by three pools based in China. This situation may damage the trust in the system, and it also carries the risk of transforming miners into an elite group that decides which transactions will be made and which

[20] Nian, L. M., and Chuen, D. L. K. (2015). Introduction to Bitcoin. Handbook Of Digital Currency. Elsevier Inc.

will not, under black market conditions. Another point where exchanges that mediate the conversion from cryptocurrencies to fiat currencies damage the decentralization of crypto currencies is that these institutions are suitable for control by the state, regulatory agencies and even private companies. The judgment to be drawn from this point is that the ideal crypto currency should have the capacity to operate independently of miners. In a mining market, it is not possible to remove transaction costs arising from intermediation. As long as the mining activity exists, the intermediary institution will continue to exist in the system, although the structure and form of intermediaries will change.

3. BLOCKCHAIN TECHNOLOGY

Tim Swanson, former director of global business development for the R3 consortium, which was formed from more than two hundred organizations interested in blockchain, said that everyone is talking about blockchain, but nobody knows what it is.[21] Indeed, there are two main difficulties in explaining blockchain. Firstly, there is no consensus even on the basic concepts of the blockchain ecosystem, which is still evolving and changing at a very high rate. Second, the multidisciplinary nature of blockchain makes it difficult to explain its content, especially at a technical level. Although the term blockchain is one of the most common uses in the literature, it is noted that the concepts of distributed ledger, shared ledger, consensus ledger, distributed database, decentralized database are often used as alternatives (and sometimes synonyms).[22] Apart from the content of the concepts in terms of language and expression, there is still no consensus on the classification of blockchain in computer science and what it includes.[23] Moreover, it is impossible to compromise not only what Bitcoin is based on and what it is called. Because there is an important problem of concept and context confusion that encompasses many elements of the blockchain ecosystem. In this regard, it should be noted in advance that it is very difficult to define a blockchain that will be accepted by all and draw the boundaries of its content. Blockchain, which is often referred to as a technology, has undoubtedly gained widespread acceptance with the

[21] Cortese, A. (2016). Blockchain technology ushers in the Internet of Value, Cisco Feature Story, https://newsroom.cisco.com/feature-content?articleId=1741667

[22] Walch, A. (2017). The Path of the Blockchain Bexicon (and the Law), Review of Banking and Financial Law, Vol. 36, pp. 719–20

[23] Rosario, N. M. (2017). What's in a Name? From Bitcoin to Blockchain to Distributed Ledgers, https://www.coindesk.com/whats-in-a-name-from-bitcoin-to-blockchain-to-distributed-ledgers;

extraordinary growth of bitcoin in the markets in 2017, and even in this context, the concepts of bitcoin and blockchains have often been used interchangeably.[24] However, from a technical point of view, blockchain is a tool, and Bitcoin is the first application made possible by this tool. Thus, there are many misunderstandings and reservations in the blockchain ecosystem.[25] The main reason for this is that the blockchain has a fragmented yet complex entity that integrates various concepts from many disciplines such as cryptography, computer science and economics, as well as the knowledge required at a technical level. From the second point of view, blockchain resembles a puzzle, which consists of many parts and can be combined in more than one way, and due to its quality of the puzzle, it generates many innovations itself, but also creates a feedback loop in which the confusion of concept and context increases with each innovation. Even though the blockchain is based on Bitcoin, it should not be confused with Bitcoin. Blockchain is the protocol that powers Bitcoin. Bitcoin is the first application developed using the blockchain protocol. In other words, it is a coincidence that digital currency was the first implementation of the blockchain. [26]In terms of historical development, Bitcoin first appeared on the scene, but the blockchain protocol on which Bitcoin was built has gained attention over time and became the mainstream. In fact, Bitcoin used neither blockchain nor distributed ledger expressions when it entered the scene. In this respect, the blockchain can also be seen as a byproduct of Bitcoin.[27]Blockchain is essentially a distributed database with certain additional features and functions. Databases that perform their tasks in the background, unnoticed by the end user, are among the most indispensable elements for the functioning of modern information technology, since databases form the backbone of every platform, website, application and online service.[28]

[24] CoinMarketCap, (2019). Bitcoin price, charts, market cap, and other metrics, https://coinmarketcap.com/currencies/bitcoin/

[25] de Leon, D. C. et. al. (2017). Blockchain: properties and misconceptions", Asia Pacific Journal of Innovation and Entrepreneurship, Vol. 11, Issue. 3, pp. 286–300

[26] Vitalik Buterin reveals Ethereum at Bitcoin Miami 2014, YouTube, (2014), https://www.youtube.com/watch?v=l9dpjN3Mwps

[27] Finck, M. (2018). Blockchain Regulation and Governance in Europe. Cambridge: Cambridge University Press. https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/A722E0522BC6C5300AA0813340BD6C04#

[28] De Filippi, P., and Wright, A. (2018). Blockchain and the Law: The Rule of Code, Harvard University Press, p. 663

Therefore, the fact that the blockchain is essentially a database does not diminish its value, but increases it exponentially. Although one of the main characteristics of a blockchain database is its distributed structure, the distinguishing feature of a blockchain is not only this distributed structure. Distributed databases, or distributed systems in general, are not a new field of computer science. In this regard, distributed database technology can be defined as a database distributed over a network of independent devices.[29] Blockchain protocol is a kind of distributed database technology and one of the best practices. Rather than introducing a new invention, blockchain creatively integrates work across multiple fields such as distributed systems, asymmetric cryptography, and consensus mechanisms. The analogy with the riddle is also true in this sense. Indeed, almost every piece of the blockchain puzzle is based on academic research from the 1980s and 1990s.[30]

The block chain was created by the original combination of these parts. When one examines the definitions of blockchain in the literature, one may notice that the focus is on distributed structure, cryptographic fundamentals, and data integrity. Blockchain, a shared and synchronized database supported by an algorithm, a decentralized database supported by a distributed computer network, a distributed ledger based on cryptographic technologies and cryptoeconomic incentives, or digital information with specific characteristics that characterize the ledger. It can be defined as a recording method.[31] On the other hand, with a technical approach, blockchain can also be defined as a data structure that provides data integrity and authentication through cryptographic functions.[32] Defining blockchain as just a database makes some of its functions inaccurately limited, while the term ledger is incompatible with the general and overarching nature of blockchain as it has a financial context.[33]

It should not be forgotten that definitions with a technical approach are true and correct in this respect, but as a phenomenon, a blockchain means much more than a data structure consisting of blocks. Blockchain has opened the door to a new paradigm in how data is processed. This was

[29] Yeoh, P. (2017). Regulatory issues in blockchain technology, Journal of Financial Regulation and Compliance, Vol. 25, Issue. 2, p. 2, doi:10.1108/JFRC-08-2016-0068

[30] Ibid, p.324

[31] Conte de Leon, D., Stalick, A. Q., and Sheldon, F. T. (2017). Blockchain: properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3), pp.286–300

[32] Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain (2. Vol.). O'Reilly. https://www.bitcoinbook.info/

[33] Buterin, V. (2015). Visions, Part 1: The Value of Blockchain Technology, Ethereum Blog, https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/.

done not only with the technical application. Therefore, if the entity, the foundations of which were first laid by Satoshi Nakamoto, is called a blockchain, it will inaccurately define it only on a technical basis. Because such a tough technical approach will limit the blockchain more than it should be. While the definition of blockchain as a technology is preferable in terms of language and expressiveness, blockchain refers to a method that uses many technologies and concepts rather than one technology. Again, the protocol used in defining the blockchain emphasizes the programmatic side, while the term network emphasizes the multiparty function. In this respect, it would be more correct to speak of blockchain as a data processing model. The concept of the model will better explain the structure of the puzzle and the flexibility of the blockchain, as well as reveal its structure, consisting of more than one technology and concept. In this case, blockchain should be defined as a method, the term ledger should not be included in the definition, it should not use a rigorous technical approach, and blockchain should not be exclusively referred to as a database or technology. At the same time, a possible definition should include irreplaceable blockchain features, but these features should be expressed in general terms, not just to define Bitcoin. In light of these explanations, blockchain can be defined as a decentralized data processing model that ensures stakeholder consensus and data integrity through cryptographic techniques and cryptoeconomic incentives.

Understanding the structure of the blockchain model and how it works is important in terms of explaining its characteristics and functions. However, the technical aspects cannot be left out when explaining how blockchain works. For this reason, the technical elements will be mentioned very superficially under the heading of the basic operation, and the main details concerning the technical issues will be covered within the technical framework in the second part of this section. It is also helpful to explain working with the most common bitcoin blockchain in order to implement the blockchain. The Bitcoin blockchain can be compared to a book, a copy of which is stored on different computers around the world.[34] Anyone can add new content to this book, and when content is added, a copy of the book is updated on all computers that have Bitcoin software installed. Unlike a book of pages, Bitcoin is organized into blocks. While the information to be added to the ledger is aggregated as a page, the transactions to be added to bitcoin are grouped together and made into a block. So, the main way blockchain works is to organize data into blocks

[34] De Filippi, P., and Wright, A. (2018). Blockchain and the Law: The Rule of Code, Harvard University Press, p.431

and create a chain from those blocks. The basic principle here is that the chain only works in stages. When new data is processed in the chain, the previously saved data is not changed, instead a new record for that data is appended to the end of the chain. In this respect, the Bitcoin blockchain can be compared to a huge ledger of checking accounts. In maintaining the current ledger, when a new debt or receivable situation arises, the previous entries in the ledger are not changed and this information about the receivable or receivable is recorded at the end of the ledger. Likewise, if John sends again 3 of the 10 bitcoins that Katie sends John to Katie, two entries are created in the blockchain according to the date and time order: First, Katie sent 10 bitcoins to John, and second, John sent 3 bitcoins to Katie. As you can see, instead of modifying the two separate records that store the balance amounts of Katie and John, as in a normal database, Katie and John transactions are recorded in the chain in chronological order, and the Katie and John balances are calculated by collecting all the transactions they previously had. fulfilled. In this way, the amount of data on the blockchain increases cumulatively and data loss on the blockchain is prevented by any new transaction. While page numbers are used to organize the content of a book, block headers serve the same function in the block chain.[35] The date and time information in the header of each block is what allows you to arrange the transactions between Katie and John in chronological order. However, the block header also contains alphanumeric text that mathematically summarizes the information in the previous block. This text can be thought of as a digital fingerprint of the previous block and hence it is specific to the content of the previous block, and even when any data in this block changes in the slightest degree, the block fingerprint is no longer saved, the letters and numbers in the text change. This way, each block in the Bitcoin blockchain has a special reference to the data fingerprint in the previous block, and thus the chain of links is formed in chronological order from the first block to the last block. For example, block 100 stores the fingerprint of block 99 and block 101 in the header of block 100. The advantage of this chain of links is that changing any block creates a domino effect in the entire chain and destroys the fingerprint references of all subsequent blocks along with it. In short, any change made to any block in a chain breaks all chains after that block. This ensures the integrity of the data in the chain.

So how does Katie send Bitcoins to John on the bitcoin blockchain? What's stopping Eda from spending Katie' Bitcoins? Blockchain can be compared to email in the sense that it allows

[35] De Filippi, P., and Wright, A. (2018). Blockchain and the Law: The Rule of Code, Harvard University Press, p.445

people to claim ownership of certain assets.[36] Today, thanks to the email protocol, we can receive messages from anyone with an email account, and as long as we have access to the Internet, we can read that message and forward it to others. Our email addresses often do not directly identify us, but act as a kind of pseudonym. However, two people cannot have the same email address because each email address is unique. In addition, each email address has a unique password, and you need to know the password to access your email account. Everyone has a public key and a private key on the Bitcoin blockchain. These keys are text made up of specific letters and numbers. The public key corresponds to the email address and the private key corresponds to the password. The only information Katie needs to get from John who wants to send bitcoin to John is his public key. However, Katy needs to use her private key that matches her public key in order to be able to send her bitcoins to John. Therefore, in order to perform transactions with bitcoins, any account must know the password of that account, in other words, the private key, which is the equivalent of the corresponding public key. It remains only to add blocks to the chain. Which of the thousands of participants in the Bitcoin blockchain will be able to add blocks to the chain and how will it be confirmed that this added block is correct, for example, there is no double-spending transaction in the block? Consensus participants of the Bitcoin blockchain with consensus protocol can add a new block to the chain, thereby agreeing on the final state of the records in the chain. For a new block added to the chain to be considered valid under the Bitcoin protocol, the block must include the answer to a mathematical puzzle that is difficult to solve but easy to verify. This answer, called proof of labor, refers to the content of the block in question and is directly related to the block fingerprint.

Therefore, be sure to solve different puzzles in each block. The participant who prepares a new block and solves the puzzle in accordance with the data in the block makes an announcement to others on the network and asks them to accept their block. Other participants asked if the transactions in the block were correct, such as whether the transaction was actually made using Katy's private key, or whether there was sufficient balance in Katy's account, and whether the puzzle was correctly answered according to transactions in the block, by others. in words, is it valid. they check. Thus, the block is added to the chain by all participants after checking its correctness and validity. Returning to the book analogy, at this stage everyone updates the book

[36] Ibid, p.396

on their computer. On the other hand, the participant who prepares the block is rewarded with a certain amount of newly minted bitcoins, depending on his contribution to the network.[37] In this way, blockchain provides continuity by rewarding those who contribute to it. Here, the longest valid chain wins according to the Bitcoin protocol, although network participants have the ability to create different block chains by dividing them into pieces. Thus, the system directs all participants to act in concert and can sustain itself with the right information if the majority is honest. Within all these explanations, a transaction on the Bitcoin blockchain can be explained in six steps:[38]

1. Katie announces on the Bitcoin network to send bitcoin to John using a transaction that she signed with her private key.
2. Network members combine Katy's transaction along with other reported transactions into a block.
3. Members of the network begin to work on finding answers to puzzles that will allow their blocks to be verified in accordance with the Bitcoin protocol. This research currently takes about 10 minutes. This means that the bitcoin sent by Katy will be credited to John's account and the new block will be added to the blockchain within 10 minutes.
4. The participant solving the puzzle related to his block announces the block prepared by him to other network participants with the answer to the puzzle.
5. Network participants check the correctness of transactions in the block and the answer to the puzzle. If the block is confirmed to be accurate, the participant who prepared it will be rewarded with a certain amount of bitcoins in exchange for their labor.
6. Network members add this accepted block to their chain and begin work on a new block based on the longest active chain announced in the network.

The blockchain ecosystem is made up of actors that play different roles in the functioning of the blockchain. In this sense, an entity can be defined as individuals or groups that interact directly or indirectly with the blockchain. Although the participants in this blockchain can change according to the structure of each blockchain, basically the participants in the blockchain ecosystem can be grouped under six functional terms: Developers, Leading Communities,

[37] Nakamoto, S. (2009). Bitcoin open source implementation of P2P currency, Satoshi Nakamoto Institute. Satoshi Nakamoto Institute. https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/3/
[38] Ibid

Network Members, Users, Agents, and Manufacturers. As a result of the functional classification of these subjects, a person or group can act as all or only one of these subjects. One of the common features of blockchain projects is that they are often developed using a free software model.[39] This means that anyone can propose to add or change code for the related blockchain software, thereby contributing to the development of the software. In such an ecosystem, the concept of a developer can be used mainly for three groups: independent developers, co-developers, and application developers. As with any software, there are developers who first wrote them for software implemented using the blockchain model. These people, who might be called self-developers, often work under the roof of the original project or organization using the blockchain model. Co-developers are people who provide code support to open source software only. The difference between self-developers and co-developers is that self-developers have some additional authority over the code or development process compared to co-developers. Because blockchain projects help protect up to billions of dollars of assets, every code change must be reviewed by experienced developers.[40]In this statement on the Bitcoin website, experienced developers can be called self-developed.

Another test that will see litmus test here is whether a developer can still provide code support for software if the blockchain project was not open source. In such protected software, if the developer still has a say in the code, then it can be called primary, if not secondary. While the main developers and co-authors contribute to the blockchain software itself, the application developers are the people who work on the applications that will be built on the blockchain. For example, software developers who code a smart contract written on the Ethereum blockchain and integrate it into Ethereum can be called application developers. These software developers are only application developers in terms of the Ethereum blockchain, as they will undoubtedly become independent developers in terms of the smart contract they have written. On the other hand, if a blockchain project is managed without a free software model, then there will be no need to distinguish between a self-employed developer and a co-developer. In this main case, application developers can be mentioned according to the nature of the blockchain.

[39] Ethereum, Licensing - Ethereum/wiki, GitHub, (2019), https://github.com/ethereum/wiki/wiki/Licensing

[40] Development - Bitcoin, Bitcoin.org, (2019), https://bitcoin.org/en/development#code-review

Technological systems are produced by society, and Castells is concerned with Internet culture. Social production feeds on culture. Using his expressions, he states that the Internet is no exception, in fact, the culture of the Internet developers shapes the Internet as a medium.[41]

According to Castells, it is impossible to understand the technological development of the Internet without understanding the communities that govern the Internet culture. Castells' social and cultural approach to the Internet seems highly relevant to the blockchain ecosystem.

In fact, the strong influence of various communities such as cryptanarchists and their cultures on the development and distribution of Bitcoin and other blockchain projects is undeniable.[42]

These pioneer communities and their cultures survive today in a wide variety of environments. Because in blockchain projects, one can observe that both developers and people who are not familiar with coding come together as a community around the project and strive to ensure that the blockchain reaches its full potential. Members of these communities discuss general issues and principles such as course, mission and project vision, as well as technical issues, and take on an important mission in terms of disseminating projects in the blockchain model and reaching end users. In this regard, perhaps the most effective blockchain-shaping player is the innovative communities and the culture they create. In addition, these communities can sometimes perform certain administrative functions by structuring them as different legal entities such as associations. While pioneering communities influence blockchain culture, administrative communities are shaping the future of the chain in this context and can act as a kind of board of directors. In this respect, it can be said that the administrative communities have a stronger concrete influence on the respective blockchains. For example, the administrative work on the Ethereum blockchain was taken over by the Ethereum Association, and Ethereum trademarks were registered in the name of this association.[43]

Network participants are people or groups that maintain the continuity of the system using the blockchain model, in other words, maintain the network. The network participants are indispensable for the blockchain, as the blockchain has a structure that is stored in a decentralized structure and is constantly updated based on consensus. In this regard, it cannot be said that a

[41] Castells, M. (2001). The Internet Galaxy. Oxford University Press

[42] Hepp, A. (2016). Pioneer communities: collective actors in deep mediatisation, Media, Culture and Society, Vol. 38, Issue. 6, pp. 918–33

[43] Trademarks, J. (2019). Stiftung Ethereum (Foundation Ethereum) Trademarks, https://trademarks.justia.com/owners/stiftung-ethereum-foundation-ethereum-3479392/

blockchain that is not a member of the network works. Because in this case, there will be no one to add new transactions to the chain and control the added blocks. In the blockchain model, although the people participating in the network are in principle in an equal position, they can perform different tasks and perform different functions on the network according to their desires.[44] In this respect, network participants can be divided into two functions: miners and validators.[45] Miners store the entire blockchain and prepare new blocks to be added to the blockchain by solving mathematical puzzles related to those blocks and seeking rewards from the system. On the other hand, there is no need to store the entire blockchain in order to participate in the network. Network participants who want to take on the task of verifying only the accuracy of transactions occurring in the blockchain will need to store only the block headers of the longest chain, that is, only a part of it. For example, almost all network participants in the Bitcoin blockchain act as validators.[46]

Users are the people who benefit most from the blockchain, and in a sense, they are its customers. However, the concept of a shopper should not lead to the conclusion that users can only be consumers. Rather, blockchain users can also be various organizations, such as companies or non-profit organizations. For example, an organization called the Ethereum Business Association was created to develop standards to enable companies to benefit from the Ethereum blockchain and meet business needs. This group includes Accenture, BBVA, Kaspersky Lab, Latham & Watkins, Microsoft and Pfizer, as well as various organizations from a wide variety of industries.

To be a blockchain user, you do not need to be a member of the network. In fact, a user who wants to buy Ether, or a merchant who wants to receive Bitcoin payments from consumers, can fulfill these requests without joining the network as a miner or validator. This is often allowed by brokers, another member of the blockchain ecosystem. While decentralization and decentralization are the main features of the blockchain model, intermediaries can arise at specific points in the ecosystem. While almost none of these intermediaries are technically required for the blockchain to operate and users can benefit from the chain, most blockchain users perform their on-chain transactions through these intermediaries. We can say that the main reason for this

[44] Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain (2. Vol.). O'Reilly. https://www.bitcoinbook.info/

[45] Bacon, J., Michels, D. J., Millard, C. and Singh, J. (2017). Blockchain Demystified. Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017

[46] Narayanan, A. and Clark, J. (2017). Bitcoin's Academic Pedigree. Communications of the ACM, 60(12), pp.36–45.

situation is that interactions with blockchains have not yet happened through user-friendly interfaces. If we draw an analogy, although today almost everyone uses an intermediary service provider such as Google, Microsoft, Yandex to manage their email accounts, the email protocol can be used without any intermediary due to its free and open source nature.[47]

Likewise, for example, in the blockchain ecosystem, users can use wallet service providers to manage exchanges and accounts to buy and sell bitcoins; Miners use mining pools to somehow insure mining activity; merchants, on the other hand, use payment service providers to securely accept cryptocurrency payments and convert to traditional currencies. In this respect, it can be said that most of the intermediaries in the blockchain ecosystem are technically voluntary intermediaries. Here we need to show the difference between brokers and application developers. When application developers write a blockchain-based application, agents use applications that do not work with the blockchain, but interact with it. For this reason, brokers do act as an intermediary between the blockchain and the user, but application developers do not have an intermediary here as their applications are already part of the blockchain itself. Thus, application developers and brokers have different functions in the ecosystem. Thanks to the miner reward mechanisms that ensure the continuity of the blockchain ecosystem, a large sector has been formed from the hardware to make mining more efficient. For example, with the increase in the number of miners on the Bitcoin network, participation in mining using conventional computers has turned into a loss of balance of income and expenses. In fact, today the bitcoin mining market is dominated by microcircuits called specialized integrated circuits (ASICs).[48]

These chips are specially optimized for Bitcoin mining and their sole purpose is to be used in Bitcoin mining. In this regard, there are companies that are exclusively engaged in the production of such chips and equipment that will be used in mining in general, and these companies have important power in the blockchain ecosystem, especially in the mining industry.[49]

[47] De Filippi, P., and Wright, A. (2018). Blockchain and the Law: The Rule of Code, Harvard University Press, p.395

[48] Ibid, p.149

[49] CoinDesk, (2018). https://www.coindesk.com/bitmain-by-the-numbers-an-inside-look-at-a-bitcoin-mining-empire

4. TYPES OF CRYPTOCURRENCIES AND THEIR ISSUES

4.1 Bitcoin

Bitcoin emerged in 2008 with an article titled User-to-User Electronic Cash System, published by an individual or group under the pseudonym Satoshi Nakamoto.[50] On January 3, 2009, Bitcoin software became open source around the world. Bitcoin was not used in trading until 2010. After that date, programmers, along with system developer Satoshi Nakamoto, revised the open source Bitcoin software and published a second version. The first Bitcoin transaction was made on May 21, 2010 by Laszlo Hanech, nicknamed Bitcoin, when he ordered a pizza for 10 thousand bitcoins, the equivalent of which at that time was $ 41.[51] Laszlo Hanets, a Florida-based software engineer, is also referred to as the developer who invented GPU-based Bitcoin mining.[52] After the economic crisis that hit South Cyprus in March 2013, when Cypriot citizens and Russians converted their very large assets to bitcoins, their value was less than $ 10, but as of April 2013, bitcoin was shining at over $ 200. dollars, also converted the yuan into bitcoin. It lost its value a lot after China took precautions and banned Bitcoin in December 2013.[53] Bitcoin, is not decentralized, not tied to any central bank or official institution, and therefore independent of any country's economy, continues to occupy the agenda of the financial world. Bitcoin, whose symbol ฿, abbreviated as BTC, allows you to transfer money in cryptocurrency from anywhere in the world with Internet access without the need for any intermediary institution. The smallest unit of cryptocurrency Bitcoin is equal to one 100 millionth part of Bitcoin.[54] Bitcoin's biggest advantage is claimed to be that it eliminates the double spending problem.[55] The concept of double spending is expressed

[50] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, p.3.
[51] Barski, C. and Wilmer, C. (2015). Bitcoin For The Befuddled, San Francisco, p.112.
[52] Vigna, P., & Casey, M. (2016). Cryptocurrency: The future of money.
[53] Nishibe, M. (2016). The Enigma of Money Gold, Central Banknotes and Bitcoin, Japan.
[54] Halaburda, H. and Sarvary, M. (2016). Beyond Bitcoin The Economics of Digital Currencies, New York 2016, s.104-108
[55] Bitcoin and Money Laundering, Developments In Banking Law. Boston University, 2016-2017, https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjE4MGrwdnYAhVREVAKHScGAtsQFggnMAA&url=https%3A%2F%2Fwww.bu.edu%2Frbfl%2Ffiles%2F2017%2F03%2FDA-13.pdf&usg=AOvVaw1cHZOX80URnsw9maXFlCtQ

as the simultaneous spending of the same funds on two buyers and is seen as a potential problem in the digital money system.[56]

Bitcoin can be bought with real money or in exchange for selling a product or service. It is also obtained through mining, which means solving complex mathematical formulas with the computing power of a computer. Anyone can join the network with any equipment and mine bitcoins. Bitcoin is made up of a protocol made up of rules that govern how the network will work, the software design that uses the protocol, computer networks, and the hardware that the software runs to receive bitcoins. Mining is billed as a core function in the governance of the Bitcoin network. Miners also play a very important role in bitcoin mining. Mining is defined as verifying transactions, avoiding double spending, collecting transaction fees, and generating money. Bitcoin mining, which allows a new block to be produced every 10 minutes, was first launched in 2009 and gave 50 bitcoins as a reward to users who found a solution through the mining process and computer systems. This reward is expected to halve every four years and end entirely in 2140, with the reward currently at 12.5 BTC. This incentive system cuts the supply of bitcoin in half by 210,000 blocks every four years. According to this table, bitcoin was initially distributed in large quantities. It is also argued that the fact that more than half of the 21 million was completed within the first six years would eventually make Bitcoin a rarity, and thus a policy similar to traditional monetary policy was adopted. When 77 bitcoin miners find a new block, they also receive the new bitcoin and any transaction fees. A widely used method of mining bitcoins is getting bitcoins using powerful video cards and their GPUs. Mining is the process of finding a number with a function on a computer and finding that special number on a computer. To do this, this is done by computers that produce a certain amount of computing power, and machines with different functions in terms of solving algorithms and energy use, such as CPU, GPU, FPGA, ASIC, which are used to get more bitcoins.[57]

Participants who secure transactions by solving a cryptographic puzzle on the blockchain are defined as miners. The mining process is related to cryptocurrencies based on the Proof-of-Work consensus mechanism. The miner uses the computing power of the computer to verify

[56] Double Spending Explained, https://academy.binance.com/en/articles/double-spending-explained
[57] Sterry, D. R. (2012). Introduction to Bitcoin Mining, A Guide Gamers, Geeks, and Everyone Else, pp.10-14.

transactions, expand the network and reward new coins. In 2009, when bitcoin first appeared, it was easier to get bitcoin by mining, and there was no need for devices that consume large amounts of energy. Over the years, as more and more users joined the system, mining became more difficult and high performance devices were used. With the use of these devices, the need arose for the use of cooling devices. Thus, while mining is not very expensive to start with, the costs are growing rapidly day by day.[58] The main idea of increasing difficulty is to try to prevent the growth of cryptocurrencies on the market in a short time and automatically adjust the difficulty level to keep the block generation rate at a certain level. This process takes place thanks to a technology called blockchain. The increase in the number of users participating in the system day by day makes it difficult to create blocks using the mining method alone. For this reason, the mining pool is a new concept; It is defined as a group of miners who come together to form a block and share the rewards earned among the miners in that group.

Figure 3. ASIC Machines Used for Mining[59]

Apart from real mining, bitcoin mining is also done through cloud mining. Cloud mining is the process of obtaining bitcoins by renting powerful hardware devices used in bitcoin

[58] Karishnan, H., Saketh, S., and Vaibhav, V. T. (2015). Cryptocurrency Mining – Transition to Cloud, International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, India, p.115

[59] Limer, E. (2013). The World's Most Powerful Computer Network Is Being Wasted on Bitcoin, https://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-504503726,

production through servers in exchange for certain conditions. The most important difference from real mining is that the various hardware devices integrated into the computer do not require any cost to mine bitcoins.[60]These servers, which were installed in cold climates such as Iceland, Washington, Utah and Sweden, are said to have turned Bitcoin mining into a large industrial business in a very short time to take advantage of low ventilation costs and cheap electricity prices.[61]

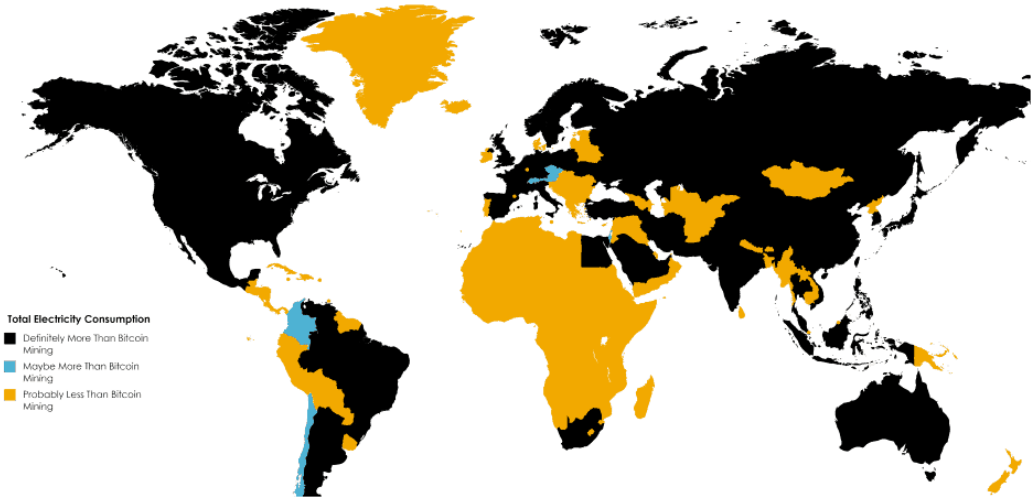
Figure 4. Cloud Mining Servers

According to research by Divesh Aggarwal, a scientist at the National University of Singapore, and colleagues; Over the next 10 years, quantum computers based on Heisenberg's uncertainty principle, one of the laws of quantum physics, will work with qubits millions of times faster than existing computer systems, instead of using the zero and one called bits of today. computers, both mining bitcoins, and it is claimed that it has identified a threat to bitcoin encryption algorithms.[62] Bitcoin is obtained through serious consumption of electricity and energy 24/7 non-stop, by a method called mining. It is known that while people earn money in exchange for the physical labor they spend, computers also use mining and processing power to get bitcoins. According to the Digiconomist Bitcoin Energy Consumption Index, as of the end of 2018, Bitcoin

[60] Karishnan, S. et. al. (2016). Cryptocurrency Mining – Transition to Cloud, International Journal of Advanced Computer Science and Applications, p.115.
[61] Vigna, P., & Casey, M. (2016). Cryptocurrency: The future of money.
[62] Quantum Computers Pose Imminent Threat to Bitcoin Security, http://www.comp.nus.edu.sg/news/news-media/2176-2017-quantum-computers/

mining consumes 55.63 to 73.12 TWh of electricity per year. It is also claimed that this means that Bitcoin mining currently uses more electricity than 175 to 181 countries around the world. It is also claimed that an estimated 94,000 kWh of electricity is consumed while mining bitcoins. The potential consumption of Bitcoin mining is said to exceed the consumption of 750 million electricity users, which is 10% of the world's population. It is also argued that even Nigeria, with the most populous population of 186 million, uses less electricity than Bitcoin mining globally. On the other hand, it is highlighted that Norway, the country with the lowest population density (5.2 million people), consumes more electricity than Bitcoin mining worldwide. It is stated that the amount of electricity consumed when mining bitcoins is equivalent to 33% in Australia, 24% in the UK, 14% in Canada and 2% in the US. Per capita electricity consumption in 66 countries is said to be lower than the amount of electricity consumed during a Bitcoin transaction. It is claimed that only 38 countries still consume more electricity than Bitcoin mining.[63]

Figure 5. Countries Consuming More or Less Electricity than Bitcoin Mining[64]



Philip Salter, head of production at the mining company, is said to have characterized mining as one of the biggest achievements of the nascent industry and stated that the mining industry has moved from China to northern countries such as Norway and Sweden. It has been argued that Western countries are seen to be safer and more stable than communist China, which is currently dominated by a great global arms race. Mining is said to have undergone a very

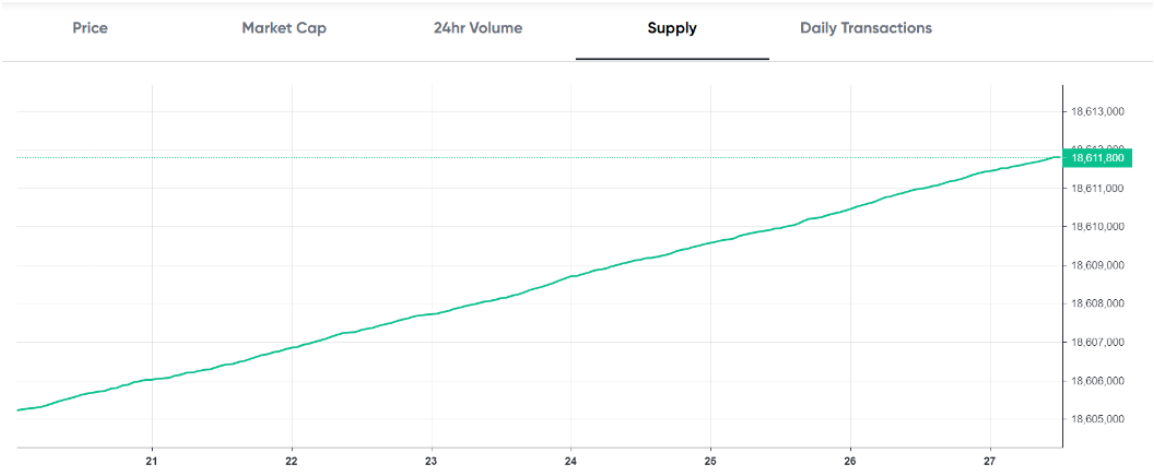
[63] Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018, https://powercompare.co.uk/bitcoin-mining-electricity-map/

[64] Https://powercompare.co.uk/bitcoin-mining-electricity-map/

important strategic shift from China to Western countries such as Sweden due to reasons such as bitcoin investors have become more public and want more critical trust. Salter's company reportedly said the Boden data center had a three-fold increase in profitability. Bitcoin has been claimed to have been referred to as a Chinese coin for years, and Ripple co-founder Chris Larsen stated that without providing any evidence, the country's authoritarian government published an article on how a country's authoritarian government could block reverse transactions on the blockchain as well. It is stated that at least 65% of cryptocurrency mining is concentrated in China, which means that the Chinese government has the ability to effectively block or cancel routing and transactions in order to control them over these protocols. It was also stated that Ripple stated that Bitcoin and Ethereum are cryptocurrencies controlled by China in a US Securities and Exchange Commission lawsuit, and these claims have drawn strong criticism from members of both communities. It is also argued that China continues to create obstacles for miners, and on the other hand, it has lost its dominant influence in the mining sector. In November 2020, users are reported to have had difficulty paying their electricity bills as they were unable to convert coins to China's official currency, the yuan. It is also reported that since September 2017, cryptocurrency trading has been banned in China. Since climate change is a very important political issue, it is also argued that Bitcoin's carbon footprint, which is referred to as energy consumption, is of concern. It is reported that in October 2020, the NYC Department of Financial Services urged crypto companies to consider the associated risks. Given that countries like Norway are environmentally friendly, it is also argued that this ongoing shift will reduce the CO2 emissions associated with Bitcoin mining.[65] The value of bitcoins is determined by the balance of supply and demand in the bitcoin market and the amount in circulation. Bitcoin is also defined as a blockchain-based distributed digital ledger. According to an article published by Satoshi Nakamoto in 2008, 21 million bitcoins will be printed by 2140. It is assumed that by this date the system will tune in, increasing or decreasing the difficulty level. The number of bitcoins currently in circulation reached 18.6 million as of February 1, 2021. At the beginning of 2017, the demand for bitcoin was growing very rapidly, and this growth can be exponentially expressed. At the time of this writing, on February 1, 2021, the value of one bitcoin exceeded $ 33,000, and its market value reached $ 626 billion.

[65] China Coin No More: Bitcoin Mining Shifting to Sweden and Norway, 27.12.2020, https://u.today/china-coin-no-more-bitcoin-mining-shifting-to-sweden-and-norway

Figure 6. Number of Bitcoins in Circulation[66]



Although it did not acquire any value until the last months of its first year, as of May 2010, the value of 1 BTC was $ 0.09 and, showing various fluctuations over time, it increased in value, reaching 33,667 US dollars, in 2021

Figure 7. Bitcoin Value Against USD[67]

As of February 2021, Bitcoin's market capitalization reached $ 626.69 billion.

[66] Money Supply, www.bitcoin.com
[67] Bitcoin Price, www.bitcoin.com

Figure 8. Bitcoin Market Capitalization[68]

Bitcoin can be bought on a wide variety of cryptocurrency exchanges and converted directly to fiat currency. Bitcoin is claimed to be one of the simplest cryptocurrencies that can be converted to fiat currency among all cryptocurrencies currently in circulation. Bitcoin is seen as a legitimate source of funding for many company owners, including big companies like Microsoft, Expedia, playboy, Virgin Galactic, LOT Polish Airlines. This is said to show that Bitcoin qualifies as a medium of exchange.[69]

4.2 Ethereum (ETH)

Developed as another cryptocurrency, Ethereum was first introduced by Vitalik Buterin and his team at the North American Bitcoin Conference on July 30, 2015. It allows the development of decentralized software protocols by developing custom software on the Ethereum blockchain database. Its developer Vitalik Buterin described Ethereum as: If we compare cryptocurrencies with valuable resources in the world and consider Bitcoin as GOLD and Litecoin as SILVER, then Ethereum is OIL. Because the technology behind Ethereum will be the powerhouse of the global internet system. Just as oil is used in many sectors and technologies around the world, the same is

[68] Market Cap, www.bitcoin.com

[69] European Parliament, (2018). Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion, July, p.33

true for Ethereum technology. This is why we call ether cryptocurrency fuel. The energy required by the Ethereum platform will be provided by Ether (ETH).

Ethereum also uses blockchain technology like Bitcoin to process its transactions, but differs from Bitcoin in several ways. Transactions in Ethereum take 14-15 seconds, which is much faster than Bitcoin. In bitcoins, this time is 10 minutes. Although the amount of bitcoins produced in bitcoin-cryptocurrency money is decreasing each time, a constant number of new coins are created in Ethereum every year. Ethereum, unlike Bitcoin, has a method of transactions by value. In Bitcoin, the most profitable is the miner who first confirms the transaction, while in Ethereum, the miner's win rate increases over time.[70]

Bitcoin and Ethereum are cryptocurrencies developed using blockchain technology. Although both cryptocurrencies are developed using the same technology, they have different systems. Bitcoin is a distributed payment system with user-to-user encryption. All transactions are transparent and open to all network users. Security is Bitcoin's top priority. The security issue is not in the external storage of data, but in the fact that the data cannot be changed unnoticed once it is created. Bitcoin uses the C ++ programming language with nearly 70 special commands. Ethereum mining was developed not only for a payment system like Bitcoin, but also for various purposes such as high security and low cost smart contracts. Ethereum, on the other hand, is designed to create smart contracts in various ways in the Ethereum system by increasing its flexibility and functionality. Ethereum was developed using seven different programming languages that are very different from the C ++ programming language used by Bitcoin. Ethereum also uses a different hashing algorithm than Bitcoin. Thus, Ethereum mining, as opposed to Bitcoin mining, is done with the GPU using the ETHASH algorithm.[71]

A hash is defined as a fingerprint of a digital file created using cryptographic hash functions. Bitcoin uses a cryptographic hash function called SHA256. When applied to a digital file, email, PDF, or Netflix movie, the SHA256 algorithm creates a single (unique) string of numbers and letters. If any changes are made to the digital file, large or small, the resulting hash

[70] European Parliament, Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead, p.13.
[71] Julianne, H. Josh, O. and John, S. (2018). Ethereum vs. Bitcoin, California, p.3.

will be completely different. The most interesting feature of SHA256 and other similar hash functions is that anyone can verify the authenticity of a digital file.[72]

Ethereum 2.0 is an improved version of the existing Ethereum blockchain, which is planned to remove recurring restrictions while highlighting the importance of Ethereum's strengths on the one hand. Seeing as the lack of scalability as the most documented shortcoming of the current Ethereum network, it is argued that the development team developed Ethereum 2.0 to implement more reliable infrastructures and increase transaction speed.[73]

Considered the second largest cryptocurrency by market value, Ethereum is said to have made the most important update in its five-year history. It is claimed that an important milestone has been reached on the road to Ethereum 2.0 called Eth2, which represents a very important milestone in the evolution of the Ethereum blockchain. Since the launch of Ethereum, the world is said to have witnessed a dramatic rise in the development of new technologies in the forum for new blockchains and decentralized applications. It is noted that the Ethereum platform provides a long-standing and solid foundation for some of the largest and most innovative developments in the distributed finance (DeFi) system. It is claimed that as the popularity of the Ethereum network grows and becomes widespread, there are scalability issues, and it aims to address these issues with the Ethereum 2.0 update, and the blockchain capacity will grow 64 times more efficiently. It is claimed that compared to the Ethereum 1.0 network, which can only support 30 transactions per second, the Ethereum 2.0 network can handle 100,000 transactions per second. With Ethereum 2.0, it is claimed to be aiming at exponential increases in the usability and functionality of the network. It is stated that one of the most exciting new features of the Ethereum 2.0 update will include the introduction of an entirely new blockchain called the Proof of Stake protocol, namely Split Chains and Flare Chain, which allows multiple transactions to be executed simultaneously. These new features are said to increase the speed, efficiency and scalability of the Ethereum network, enabling better transactions and thus preventing existing congestion issues. The split chains are claimed to have similar functions to the blockchain, but that this split chain contains only a portion of the blockchain. Split chaining is said to allow nodes to control network segments. It is claimed that

[72] Virtual Currencies Mining the Possibilities, Allen&Overy, 2015, p.4.
[73] What is Ethereum 2.0? (Release, Roadmap, Phases), https://www.benzinga.com/markets/cryptocurrency/20/11/18489382/what-is-ethereum-2-0-release-roadmap-phases

the Ethereum 2.0 network will create 64 split chains, which will provide 64 times the volume of transactions on the network. The Flare Chain is claimed to be the central component of the Ethereum 2.0 network. This new blockchain is said to allow information to be exchanged between parts and maintains parallel, parallel chains. It is also stated that shards and beacon chains are needed to improve scalability on the network. It is claimed that each of the nodes used to access the Ethereum network contains a copy of all transactions that have occurred on the network so far.[74]

4.3 Ripple, XRP (XRP)

Following the worldwide success of Bitcoin, a large number of altcoins began to appear and continue to appear. Ripple is not an alternative cryptocurrency like Bitcoin, it emerged in 2012 as a protocol that defines the transfer of cryptocurrencies. Although it originated from an open source distributed protocol, its current development is carried out only at Ripple Labs. Its production is capped at 100 billion Ripple.[75] The Ripple protocol, which is a cryptocurrency that does not have blockchain technology but instead uses a global shared ledger, is mainly used by corporate entities such as large banks and the business world. It is a cryptocurrency that Google invests and has its own algorithm for transferring money to the end user. Unlike the traditional financial system, Ripple is a network protocol that allows secure transactions from anywhere in the world, in any currency, at any time. Unlike Bitcoin, Ripple does not mine. Ripple has its own algorithm. Ripple allows you to conduct transactions in a shorter time frame and with lower transaction fees compared to Bitcoin.

After the development of Ripple, the inventors of Ripple also developed the XRP cryptocurrency. XRP is described as an intermediate currency designed to make international payments to financial institutions faster and cheaper than today's global payment networks such as banks. XRP can process over 1,500 transactions per second, according to Ripple. Originally developed as a startup, Ripple is said to have been adopted by many cryptocurrency users in a short time. Ripple (XRP) is allegedly not based on Proof of Work or Proof of Security, it has its own dedicated protocols for verifying the validity of transactions. It is very important to understand

[74] What is Ethereum 2.0? Overview, Features and Price Implications, https://www.diginex.com/insights/what-is-ethereum-2-0-overview-features-and-price-implications/

[75] Frederik, A., Ghassan, O. K., Avikarsha, M. and Franck, Y. (2015). Ripple: Overview and Outlook, pp.2-3.

the difference between XRP, Ripple and RippleNet. XRP is a currency that powers the RippleNet digital payment platform on a database called the XRP Ledger. RippleNet, on the other hand, is an open source XRP ledger based on a distributed ledger database rather than blockchain. The RippleNet payment platform is claimed to be a platform that allows real-time global money transfers. Thanks to the transparency and semi-anonymous features of Bitcoin, it can be argued that transactions can track everything on the network, revealing the concept of confidential cryptocurrency money. Confidential cryptocurrencies allow the transfer of transactions between people in a distributed manner using blockchain technology, ensuring confidentiality and anonymity. We can say that cryptocurrencies that provide complete anonymity are becoming more and more attractive for cryptocurrency users who want to conduct their business in a confidential environment, and the trend towards using these cryptocurrencies is increasing. It can be argued that the full anonymity function of confidential cryptocurrencies, due to their nature, will make money laundering and illegal activities more accessible and may pose a threat to economic security, and it can be argued that governments will have to approach these cryptocurrencies more. carefully. In the cryptocurrency ecosystem, cryptocurrencies have been developed with a high degree of privacy. Some of the widely known and used privacy cryptocurrencies are summarized below.

4.4. Monero (XMR)

Monero, another cryptocurrency developed after Bitcoin, does not use a public ledger of transactions, unlike Bitcoin, and claims that its transactions are completely private. It is alleged that based on the adaptation of the CyptoNote protocol, one-time signatures and secret addresses are used, which makes the blockchain opaque. In addition, developers continue to work on the Invisible Internet Project (I2P) integration to hide IP addresses involved in transactions. With the privacy statements in mind, we will observe how this payment structure is used for anything from stolen data or fraudulent transactions to DDoS attacks or data cleansing programs. In August 2016, AlphaBay and Oasis, both dark internet markets, announced that they would start supporting Monero as a source of payments. The next month, Monero's value increased 669%. The market value of Monero has grown from $ 5 million to $ 185 million in 2016. However, Monero has also

been incorporated into the CryptoKingdom massively multiplayer online RPG market and has been adopted by the growing consortia of the dark internet and pure gambling.[76]

Monero (XMR) is defined as an open source P2P-based cryptocurrency known as the CryptoNote PoW algorithm, which targets private and censorship-protected transactions, announced to the public in April 2014. It was specially designed to enable Monero users to carry out their transactions in complete confidentiality. Monero specifically uses cryptography to protect send and receive addresses and transaction amounts. Monero (XRM) is considered fully refundable. This means that two Monero units can always be exchanged and certain Monero units cannot be blacklisted by traders or exchanges due to their merger in previous transactions.

Unavailable cryptocurrencies like Bitcoin and Litecoin could theoretically be blacklisted. If in the past it was used in illegal activities, this information will forever remain on the blockchain. Monero runs on a contactless blockchain like Bitcoin. It has the ability to join the network without the need for approval by any central administrator. Monero can be directly converted to fiat currency through a large number of cryptocurrency exchanges. Transparent transactions like the Bitcoin and Ethereum blockchain can be openly verified and tracked by anyone at any time. While this is difficult, in practice, the send and receive addresses for such transactions can be linked to the person's real identity. But with Monero, things are a little different, and Monero positions itself as a safe, private and untraceable cryptocurrency. Monero enforces this high standard of anonymity through two methods called Ring Confidential Transactions (RingCT) and Private Addresses. RingCT consists of a combination of a method, expressed as the concept of confidential transactions in the crypto community, and ring signature methods. Ring signatures combine user account keys from public keys obtained from the Monero blockchain, which means that outside observers cannot associate the signature with the user. Along with private addresses, Monero allows users to hide the identity of the sender and recipient. Confidential transactions provide additional privacy by hiding the amount of each transaction. It contains cryptographic proof that the input values are the same as the sum of the output values, without revealing the real numbers. Besides RingCT, Monero also uses private addressing. Private addresses are generated randomly for each transaction by the sender on behalf of the recipient. All payments sent to the recipient are

[76] Benjamin, B. (2016). 2016 State of the Dark Web, Akamai, Threat Advisory, p.6

routed through these addresses to ensure there is no connection between the sender and recipient addresses in the blockchain.[77]

4.5 Tether (USDT)

Tether is said to have been first launched in July 2014 under the name RealCoin, and in November it was renamed Tether by Hong Kong-based Tether Limited, which is responsible for maintaining the fiat currency reserve, and began trading in February. 2015 Tether is claimed to be defined as a cryptocurrency developed using the blockchain-based Omni Layer protocol, which is backed by an equivalent number of traditional fiat currencies such as the dollar, euro or Japanese yen that are stored in a specific bank account. Tether tokens, which are the native tokens of the Tether network, are said to be traded under the symbol USDT. Tether is said to have evolved into a new stable cryptocurrency that aims to keep the value of the cryptocurrency stable, as opposed to the wide fluctuations seen in other mainstream cryptocurrencies such as Bitcoin and Ethereum. Tether's stable cryptocurrency feature is said to allow it to be used as a medium of exchange and store of value rather than being used as a speculative investment vehicle. Tether is said to be specifically designed to bridge the gap between fiat currencies and cryptocurrencies and offer users stability, transparency, and low transaction fees. Its manufacturer, Tether Limited, is said to state that the value of each Tether in circulation is $ 1. With the release of Tether, which is mentioned in the stable money category, it is also stated that it can be converted, transferred, stored and spent in fiat currencies such as Bitcoin or any other cryptocurrency, subject to Tether Limited's terms of service. It is argued that the fiat currency in the reserve acquires the characteristics of crypto-money, and its value is constantly dependent on the fiat currency. It is also claimed that Tether is located on the Bitcoin blockchain instead of the less developed / tested altcoin blockchain. It is claimed that Tether can be used in an end-to-end, semi-anonymous, distributed and cryptographically secure environment like Bitcoin. It is also stated that Tether can be integrated into exchanges and wallets as easily as Bitcoin or other cryptocurrencies.[78]

---

[77] European Parliament, Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion, July 2018, pp.45-46

[78] Frankenfield, A. (2019). Tether (USDT), https://www.investopedia.com/terms/t/tether-usdt.asp#:~:text=Tether%20is%20a%20blockchain%2Dbased,trade%20under%20the%20USDT%20symbol

In April 2019, the New York attorney general accused Tether of covering $ 850 million in losses from the Bifinex cryptocurrency exchange. Tether is said to consider this accusation as malicious intent and false claims. The New York attorney general has reportedly also filed a lawsuit against Bitfinex and Tether's parent company, iFinex. It is noted that Judge Joel Cohen extended the deadline by another 90 days during the May 2019 injunction because he was not ready to make a final decision to continue or dismiss the case. It is also stated that in August 2019, the New York Attorney General also presented further evidence, claiming that Bitfinex and Tether have served their clients in New York for longer than they claimed, except for the cover-up of Bitfinex and Tether in losses of $ 850 million. ... The NYAG was later alleged to have described iFinex's actions as an improper attempt to obstruct a judicial investigation. The case reportedly took an interesting turn in September 2020 after Judge Cohen decided that Tether and Bitfinex should prepare documents explaining their financial relationship. On December 9, 2020, Attorney General Laetitia James reportedly submitted a document requesting the extension to be postponed until January 15. In addition to announcing iFinex's activities on Bitfinex related to USDT and Bitcoin, it is also stated that Tether should prepare a document detailing the issuance and redemption of USDT stablecoins.[79] In April 2019, New York Attorney General Laetitia James allegedly accused iFinex, the parent company of Tether Limited and cryptocurrency exchange operator Bitfinex, of hiding $ 850 million in mutual funds and institutional funds from investors. The court records indicate that these funds were transferred to the Panamanian Crypto Capital Corp without any contract or agreement to fulfill withdrawal requests from its clients.

4.6 Dash (DASH)

Formerly known as Darkcoin, Dash is defined as an open source P2P cryptocurrency focused on privacy. It first appeared in January 2014 based on the X11 Proof of Work (PoW) algorithm. What sets Dash apart from other cryptocurrencies is that Dash has a two-tier network. The Dash blockchain, called masternodes, is secure and proof of work is done by miners. A masternode is a server connected to the Dash network that guarantees minimal performance and functionality for specific tasks related to PrivateSend and InstantSend, concepts related to Dash anonymity, and instant transaction features. Traditional cryptocurrencies can take a long time to trade. This is

[79] Akolkar, B. and Sharma, S. (2021). Tether (USDT) Conspiracy Tosses Again As We Arrive at The D-Day of January 15, https://coingape.com/tether-usdt-conspiracy-tosses-again-as-we-arrive-at-the-d-day-of-january-15/

because transactions are irreversible and at the same time enough blocks must go through to avoid double payment situations. It solves this problem with the Dash masternode feature. Dash is said to compete with near-instant transaction systems such as credit cards. Dash also runs on a contactless blockchain like Monero. Anyone can join the network without the approval of the central administrator. Dash can be directly converted to fiat currency through various cryptocurrency exchanges. Like the Bitcoin blockchain, the Dash blockchain is transparent by default, which means that transactions can always be openly verified and tracked on the blockchain. Dash also offers its users the ability to use the PrivateSend feature to ensure true financial privacy. PrivateSend hides the source of its users' funds through a technique known as scrambling.[80]

5. CRYPTOCURRENCY MARKET RISKS

The use of cryptocurrencies as the newest form of money entails a number of risks, which can be conditionally divided into three blocks: legal, economic (financial) and technical.

5.1 Legal risks of cryptocurrency functioning

The lack of legislation in the field of regulation of the crypto market is due to the fact that society itself does not yet keep up with the too rapid development of information technologies, and at the same time with the development of the crypto market: cryptocurrency is still too progressive technology for both the majority of consumers (population) and for regulators, national governments. At the international level, the problem of the need to regulate cryptocurrencies was first raised back in mid-2014 by the FATF. However, even at the national level, a unified position on the regulation of the crypto market and cryptocurrency activities has not yet been developed. Moreover, the national regulation of the crypto market and crypto activity is dynamically developing and changing rapidly. In general, there is a global trend, regardless of what the attitude towards cryptocurrencies has been since their inception: states are trying to avoid a complete ban

[80] Ibid

on the use of cryptocurrencies and, as part of this, seek to control the cryptocurrency market, equating cryptocurrencies with virtual money.[81]

The most striking example is China, which in one decade went from completely banning cryptocurrencies to developing its own national cryptocurrency (CVCB) in 2020 - the cryptoyuan. The United States today occupies a leading position in terms of the volume of the cryptocurrency market and exchange trading of cryptocurrencies, which is largely due to the fact that American legislation is generally loyal to the functioning of the cryptocurrency market and the entire cryptoindustry. However, at the state level, a unified position has not yet been developed in relation to the regulation of the crypto industry - in some states it is regulated and companies need to obtain an appropriate license to carry out cryptocurrency activities, while in others it is prohibited. This is largely due to the fact that the US legal system is built on the basis of judicial precedent and at the state level there is no uniform position among judges in relation to cryptocurrencies and cryptocurrency activities. In this regard, it is important to mention Venezuela, which was the first in the world to introduce the national cryptocurrency "Petro" - in 2018.[82]

It should be noted that the main reason for its introduction was an attempt to overcome the most severe socio-economic crisis caused by a number of reasons, which should be attributed to: firstly, the introduction by the United States of sanctions that prevent the country from issuing debt obligations or refinancing debts, and a ban on the use of the dollar; secondly, in order to maintain the national economy and attract foreign currency, Venezuela was forced to pursue a policy of devaluation of the national currency, which led to a severe shortage of cash currency. As a result, the system of monetary circulation was almost completely destroyed in the country and, accordingly, the opportunities for participation in international economic relations were significantly limited. Accordingly, the introduction of the state national cryptocurrency allowed the country not only to stabilize the socio-economic situation and reduce the severity of the crisis, but also to improve the country's economy, in particular, it was possible to attract foreign investment in the absence of access to international loans. Moreover, the Petro cryptocurrency

[81] Sotiropoulou, A. and Ligot, S. (2019). Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?. European Company and Financial Law Review. 16. 652-676. 10.1515/ecfr-2019-0023.

[82] Herrera, A. I. and Hunter, T. (2018). Oil as Currency: Venezuela's Petro, a New 'Oil Pattern'?. SSRN Electronic Journal. 10.2139/ssrn.3291272.

today functions quite effectively as a national payment system, becoming a kind of element in a completely new financial system of the country. However, it is important to note. The introduction of Petro also had negative consequences: almost immediately, a significant increase in the number of illegal transactions began to be recorded and, as a result, the country turned into an important link in drug trafficking.[83]

Thus, in the absence of a full-fledged legislative framework and based on the very essence of cryptocurrencies as a new form of money, anonymity and the impossibility of tracking committed crypto transactions, illegal cryptocurrency transfers through an international platform, illegal drug trade, become possible. Therefore, in order to protect users and prevent money laundering and terrorist financing, states are increasingly beginning to actively amend the national legal system today.

5.2 Economic risks of cryptocurrency functioning

This block of risks of the functioning of cryptocurrencies includes the following. First, the lack of commercial acceptance of cryptocurrencies and the collapse of the crypto market. Venezuela and China are some of the most striking examples of cryptocurrency acceptance. For example, in Venezuela, for several years now, Petro has been paying pensions and salaries to civil servants. Moreover, one of the most powerful state-owned oil corporations (PDVSA) has already completely switched to settlements in the national cryptocurrency.[84] China launched its own national blockchain platform BSN in April 2020, and testing of its state cryptocurrency, DCEP, began on April 15. In June 2020, the Beijing Blockchain Innovation Development Plan for 2020-2022 was published, according to which Beijing should become the world's largest blockchain hub. To do this, over the next two years, it is planned to integrate dozens of blockchain innovations into the economy and infrastructure of the city, and then use it when registering real estate transactions, for tax purposes, etc.

However, in a number of countries, for example, in Egypt, any types of crypto-operations are strictly prohibited as contrary to the foundations of Islam. In general, in most countries of the

[83] Ibid

[84] Mosakova, E.A. (2002). National cryptocurrency as Venezuela's economic development factor in the 21st century, Iberoamérica. no. 1. pp. 160-176.

world, the scope of cryptocurrencies is still significantly limited - a number of countries do not accept them for payment. As a result, the share of cryptocurrencies in the total amount of funds is still insignificant and is at the level of less than 1%.[85]

Secondly, the high volatility of the exchange rate. Most modern cryptocurrencies are decentralized, which means there is no single emission center, and therefore no property security for the transactions. Moreover, the establishment of the rate of cryptocurrencies is carried out only on the basis of the market interaction of supply and demand. The increased demand for cryptocurrency is due to significant interest in the new instrument and, accordingly, has a significant speculative component, which in turn creates opportunities for cryptocurrency manipulation. Accordingly, financial transactions with cryptocurrencies are not controlled or regulated by government agencies, so they pose a significant financial risk for investors and the entire crypto market. Note that Bill Gates spoke about the high speculative component of cryptocurrencies for long-term investment a few years ago.[86]

A number of scientists also write about this, emphasizing that today cryptocurrencies are still used mainly for speculation and therefore are to a small extent integrated into the global financial system. Thus, S. Amus, D. Bauer and K. Hong note that this will be a significant constraining factor for their development, and as a result, cryptocurrencies will not be able to compete with traditional money.[87] Third, bankruptcy and / or closure of cryptocurrency exchanges. So, over the past 5 years, about half of crypto exchanges have closed or gone bankrupt. At the same time, as a rule, users did not have time to withdraw money from their accounts and, accordingly, cryptocurrencies disappeared. Of course, in order to maintain their reputation, many exchanges seek to recover losses, however, this is not always possible. A positive example is the bankruptcy of Bitfinex in 2018, which was able to compensate its customers. Fourth, the possibility of using cryptocurrencies as financial pyramids, which is a significant threat to the economic

[85] Shetewy, N., Ait, L. J., and Li, J.-J. (2019). Challenges of the Bitcoin in the Arabic Countries.

[86] Bill Gates: I would short bitcoin if I could. CNBC. 07.05.2018: https://www.cnbc.com/2018/05/07/bill-gates-i-would-short-bitcoin-if-i-could.html.

[87] Baur, D., Hong, K., and Lee, A. (2018). Bitcoin: Medium of exchange or speculative assets?, Journal of International Financial Markets, Institutions and Money. № 54. pp. 177-189.

security of the country as a whole, as well as to its individual individuals.[88]So, J. Stiglitz a few years ago spoke about the high degree of success of cryptocurrencies as a new form of money solely because of their significant potential for the implementation of fraudulent and fraudulent schemes, the construction of financial crypto pyramids.[89] Today, there are two main schemes for the operation of crypto pyramids:

1. Fake cloud mining. So, in the case of private mining, it may turn out that new miners are dancing to the previous ones, but real mining does not take place. Payments for mining themselves are carried out, but only until the influx of "new miners" is reduced. After that, the activities of the company are terminated and the funds disappear.

2. Investments. The organizers of the crypto pyramids promise higher interest rates and an increase in the price of the cryptocurrency itself in the future. Initially, depositors consistently receive their inflated interest income. However, with a repeated investment, which, as a rule, turns out to be more significant in value terms, it turns out to be impossible to withdraw money from the account. After that, as in the previous scheme, the activities of the company are terminated, and the funds disappear.

Note that in the case of crypto pyramids, the greatest threat is to attract user funds, since they are withdrawn from the real economic turnover, which negatively affects the development of the economy. And in the case of a significant scale of the crypto pyramid, one can even talk about a slowdown in the pace of economic development of the region and the country. Moreover, if money is transferred to accounts in foreign banks or to crypto accounts, then there is an outflow of capital from the country.

Fifth, opportunities for tax evasion, which is due to both the anonymity of the transactions and an unlimited number of cryptocurrency issuers, which makes it possible for users to hide from taxes; and significant differences in the field of legislative regulation of the crypto market and

[88] Hu, J., Luo, Q., and Zhang, J. (2020). The Fluctuations of Bitcoin Price during the Hacks. 3. pp. 10-20. 10.33422/ijarme.v3i1.278.

[89] Costelloe, K. (2017). Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says: https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd

crypto activity in the countries of the world. The biggest differences in the definition of cryptocurrencies are in the framework of indirect taxation.[90] However, since 2020, in a number of countries around the world in the EU, Switzerland, UK, Australia, Singapore, Japan, cryptocurrency transactions are no longer subject to indirect taxes, albeit for completely different reasons. Moreover, there is no single approach to the concept of cryptocurrencies for tax regulation, incl. even within the same country. So, in England, for example, for the collection of taxes on income from individuals, they are defined as property, and for the collection of VAT - as currency; in Japan - within the framework of sales tax, they are classified as currency and are not subject to taxation, and for the collection of taxes on income from individuals - as income from the ownership of property.

5.3 Technical risks of cryptocurrency functioning

First, there is the risk of losing private keys - if you lose the secret code, you lose full access to all cryptocurrencies that are in the wallet. In fact, it means losing your real wallet with all the cash in it. Secondly, the inability to cancel the transaction. In blockchain technology, it is impossible to cancel a completed transaction, incl. if it is committed erroneously, the decentralized blockchain system does not allow changing the data already entered in the register. Thirdly, cybersecurity in the field of cryptocurrency functioning is a key strategic and systemic problem both for the government, connected in many respects with new digital platforms and currencies, and for the population.

When looking at cybersecurity at the user level, there is a significant risk that cryptocurrencies could be stolen. Moreover, today there are malicious programs that are aimed at performing hidden crypto mining. At the same time, it is not even required to infect a computer with a virus or install a program - today mining is even integrated into sites, for example, for downloading audio and video.[91] Therefore, within the framework of increasing cybersecurity, it seems appropriate to regulate and control the circulation of cryptocurrencies both within countries

[90] Kochergin, D.A. (2020). Pokrovskaya N.V. International experience in taxation of cryptoassets, Economic Journal of the Higher School of Economics, no. 24 (1). S. 53-84

[91] Zimba, A., Wang, Z., Mulenga, M., and Odongo, N. (2018). Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. Journal of Computer Information Systems. 60. 1-12. 10.1080/08874417.2018.1477076.

and at the international level. At the state level, there are also a number of problems in cybersecurity in connection with the functioning of cryptocurrencies. In particular, investigating cybercrime is problematic for a number of reasons: First, cybercriminals tend to operate on the Darknet. Secondly, the disclosure of such crimes necessitates cooperation of the relevant authorities at the international level, which at this stage is not yet possible due to the ambiguity of the approaches of national governments even to issues of understanding the essence of cryptocurrencies.

6. LITERATURE REVIEW

Studies have been conducted to assess the value of bitcoins and cryptocurrencies. Specifically, there is research on Bitcoin's monetary characteristics or whether it is more similar to commodity money such as digital gold in terms of price in Bitcoin research. Below are some examples of these studies.

Li and Wang (2017) conducted a theoretical empirical study to determine the bitcoin exchange rate (versus the US dollar), taking into account both technological and economic factors. To solve the problem of joint integration in a combination of stationary and non-stationary time series, the estimation uses a distributed lag autoregressive model using the bounds checking method. Gox is one of the largest bitcoin exchanges. According to the analysis, in the short term, the bitcoin exchange rate is adjusted to reflect changes in fundamental economic and market conditions. The long-term bitcoin exchange rate is more sensitive to fundamentals and the Gox has closed.[92]

Tasca et al. (2018) sought to determine the interdependence of economic entities that use the Bitcoin payment network to internally transfer digital currency among themselves. this was done by defining and combining the minimum units of bitcoin identity, which are addresses, with units called super clusters. These clusters are tagged using a new method to make them economically anonymous. Finally, the study describes the dynamics of how these clusters behave over time. As a result of the study, it is clear that there are different models of transaction flow for

[92] Li, X., and Wang, C. A. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision Support Systems, 95, pp. 49-60.

subjects in each business category. For example, flows between traders and exchanges averaged about 20 BTC at runtime, with traders buying and selling on average every 11 days.[93]

Shahzad et al. (2019) discuss whether Bitcoin offers a safe property for stock market trading in extreme market conditions and whether such a property is the same or different from gold and the general commodity index. The article proposes a new definition of a strong and weak safe harbor in a two-dimensional crossover approach. This definition takes into account the lowest scores of both the safe-haven asset and the stock market index. The sample period is July 19, 2010 to February 22, 2018, with a focus on a variety of stock market indices including the United States, China, and other advanced and emerging economies. The main results show that every bitcoin, gold and commodity index can be seen as a weak haven asset in some cases. It also shows that the role of refuge that Bitcoin, gold, and commodities play change over time and differ between the stock market indices studied.[94]

In their work, Javaron and Wright (2018) sought to analyze the structure of these networks, focusing on Bitcoin and Bitcoin Cash. In particular, the latter derives from the former and creates a new cryptocurrency. In particular, the global structures of these networks are analyzed and an attempt is made to assess whether they have behavior in a small world. The results show that the two networks have some topological similarities, and some generative models can be accepted as preferred or most enriching for representing their evolution. In particular, even if both networks are peer-to-peer, parameters such as matching can be useful, for example, to separate nodes.[95]

According to Hendrickson (2016), while the recent spread of bitcoin is seen as a boon to users, it could pose problems for governments. Because of this, some governments are taking steps to ban or discourage the use of bitcoins. In a model with internal fit and random consumption preferences, this study examines the multi-monetary balance of bitcoin with the official currency.

[93] Tasca, P., Hayes, A., and Liu, S. (2018). The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships. The Journal of Risk Finance, 19(2), pp. 94-126.
[94] Shahzad, S. J. H., Bouri, E., and Lucey, B. (2019). Is Bitcoin a better safe-haven investment than gold and commodities?. International Review of Financial Analysis. In Press.
[95] Javarone, M. A., and Wright, C. S. (2018). From Bitcoin to Bitcoin Cash: a network analysis. 1804.02350. pp. 1-5.

Such a policy seems to be difficult to enforce if some users finally choose Bitcoin because it can interfere with other users holding the official currency during the matchmaking process.[96]

In their article, Ciaian and Rajcaniova (2016) identify and analyze the characteristics of Bitcoin that can facilitate the transformation of Bitcoin into a global currency, as well as those that may impede the use of Bitcoin as a medium of exchange, unit of account and store of value, and compare Bitcoin with standard currencies. Of all the features analyzed, Bitcoin's extreme price volatility stands out the most when compared to standard currencies. To understand the reasons for this extreme price swings, an attempt is made to identify the driving forces behind Bitcoin pricing and assess their importance from an economic point of view. It applies time series analytical engines to daily data for the 2009-2014 period. The forecast results show that indicators of Bitcoin's attractiveness are the strongest factors influencing the price of Bitcoin, followed by market forces. In contrast, macro financial developments do not determine the price of bitcoins in the long run. the results show that Bitcoin cannot compete with standard currencies as long as Bitcoin's price is mainly driven by speculative investment.[97]

Hayes (2017) sought to identify possible determinants of the formation of the value of cryptocurrencies, including bitcoin. With Bitcoin becoming more popular, it becomes more and more important to try to understand the factors that influence value creation. All bitcoins in existence today are valued at about $ 7 billion, with the relative value of $ 60 million changing from hand to hand every day. There has been a booming but dynamic bitcoin market that has grown rapidly over the past few years, and the recognition of digital currencies as a thriving asset class. There is not only an exchange and OTC market for bitcoin and other digital currencies, but also an emerging derivatives market. The study uses a regression model that identifies the three main drivers of cryptocurrency value, using cross-sectional empirical data examining 66 of the most widely used cryptocurrencies.[98]

---

[96] Hendrickson, J. R., Hogan, T. L., and Luther, W. J. (2016). The political economy of bitcoin. Economic Inquiry, 54(2), pp. 925-939.

[97] Ciaian, P., and Rajcaniova, M. (2016). The digital agenda of virtual currencies: Can BitCoin become a global currency?. Information Systems and e-Business Management, 14(4), pp. 883-919.

[98] Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. Telematics and Informatics, 34(7), pp. 1308-1321.

Lischke and Fabian (2016) study the economics and transactional network in the first four years of the decentralized digital currency Bitcoin. The goal is to get an idea of the evolution of the Bitcoin economy in the first four years. To do this, a new integrated dataset is created and analyzed that enriches the data on the Bitcoin blockchain with non-networked data such as business categories and geographic locations. Our analysis shows the major bitcoin businesses and markets. The results provide insight into the distribution of firms across countries and how firms have developed over time. The study also shows that there is a gaming network with very small transactions. There may also be regional differences in adoption and job allocation. In network analysis, the small world phenomenon has been investigated and validated for several units of the Bitcoin network.[99]

In his article, Morisse (2015) explores cryptocurrencies and bitcoin within the literature. This study summarizes the key concepts of 42 articles. Although cryptocurrency research has yet to reach information systems, the article shows that there is great potential for multifaceted research, from developing protocols to developing alternative digital currency schemes. Cryptocurrencies are a fundamental digital artifact and are a rich phenomenon based on the interweaving of technological artifacts and social contexts. At the end of this literature review, some clear research gaps are discussed, such as new cryptocurrency-based business models or the impact of culture on cryptocurrencies and bitcoin.[100]

Bohme et al. (2015) presented design principles and features of the Bitcoin virtual currency platform to a non-technical audience. It looks at its past, present and future use and identifies risks and regulatory challenges as Bitcoin interacts with the traditional financial system and the real economy. Bitcoin is an online communication protocol that simplifies the use of virtual currency, including electronic payments. Since its founding in 2009 by an anonymous development group, Bitcoin has processed approximately 62.5 million transactions on 109 million accounts. As of

[99] Lischke, M., and Fabian, B. (2016). Analyzing the bitcoin network: The first four years. Future Internet, 8(1), pp. 7-47.
[100] Morisse, M. (2015). Cryptocurrencies and bitcoin: Charting the research landscape. Twenty-first Americas Conference on Information Systems, Puerto Rico. pp. 1-16.

March 2015, the daily trading volume was approximately 200,000 bitcoins, and the combined market capitalization of all bitcoins in circulation was $ 3.5 billion.[101]

According to Werner (2016), the Bitcoin ecosystem has grown significantly in recent years. While the main sectors for growth and venture capital funding are the Bitcoin ecosystem itself and the financial services infrastructure, there has recently been development in sectors other than financial services. This study categorizes a venture capital-backed startup ecosystem and presents its evolution over time. Thus, it identifies interesting sectors, namely digital assets, markets and notary services. Each sector is further subdivided and features six representative venture capital-backed startups with extensive case studies. It examines the key innovations and features of Bitcoin on which they are based. Finally, their destructive potential is critically discussed in the study.[102]

Akins et al. (2014) examine current bitcoin laws as well as proposed methods for applying current federal income tax laws to a virtual economy. It also explains virtual currencies and the role of Bitcoin as a virtual currency, its origins and how the Bitcoin system works. He then reviews the current tax laws and regulations that should be valid for Bitcoin in general, and presents several relevant legal sources that address Bitcoin's regulation in general. Finally, it analyzes the possible federal income tax implications of various bitcoin transactions and provides guidance on the appropriate federal tax regime for these transactions.[103]

Kostakis and Giotitsas (2014) explore the political economy of the Bitcoin ecosystem. In particular, the emergence, nature, dynamics, advantages and disadvantages of digital currency are considered. It is argued that Bitcoin, which is a really interesting experiment, is an example of diffuse capitalism and should be seen primarily as a technological innovation. Rather than offering practical answers and solutions to current views on the financial crisis, Bitcoin offers several

[101] Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), pp. 213-238.
[102] Wörner, D., Von Bomhard, T., Schreier, Y. P., and Bilgeri, D. (2016). The Bitcoin ecosystem: disruption beyond financial services?. Twenty-Fourth European Conference on Information Systems (ECIS), pp. 1-16.
[103] Akins, B. W., Chapman, J. L., and Gordon, J. M. (2014). A whole new world: Income tax considerations of the Bitcoin economy. Pitt. Tax Rev., 12, pp. 25-58.

helpful and timely questions about the principles and foundations of dominant political economy.[104]

Weber (2014) evaluates the claims of the Bitcoin virtual money and payments project to provide an answer to the current money and payment system legitimacy crisis. The article examines virtual currency and the Bitcoin payment project as a critical practical form of current money and payment system. First, the study presents the main features of Bitcoin.[105]

Kroll et al. (2013) view the gaming aspect of Bitcoin as a consensus. A key design feature of Bitcoin is the mining engine, in which participants spend resources on solving computational problems to collect rewards. This mechanism protects Bitcoin from certain technical problems, such as inconsistencies in the data structure of the system's distributed log. The study explores the economics of bitcoin mining and the question of whether the bitcoin protocol can resist attacks if participants act according to their own incentives. They show that there is a Nash equilibrium in which all players behave according to the Bitcoin reference implementation, otherwise there are multiple equilibria in which they operate. That is, they argue that Bitcoin can damage the system from the outside and bring down the currency.[106]

Seetharaman et al. (2017) emphasized that if the lack of regulation of Bitcoin is addressed, it will even affect the US dollar, which is a sovereign reserve currency, in their studies where they analyze a partial least squares model.[107]

Luther and White (2014), in their study, wondering if bitcoin could be the main currency or not, stated that the hardness of the supply of bitcoins leads to a change in its value relative to traditional currencies. They also proposed initiatives that will allow Bitcoin to become a more

[104] Kostakis, V., and Giotitsas, C. (2014). The (A) political economy of Bitcoin. TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, 12(2), pp. 431-440.
[105] Kostakis, V., and Giotitsas, C. (2014). The (A) political economy of Bitcoin. TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, 12(2), pp. 431-440.
[106] Kroll, J. A., Davey, I. C., and Felten, E. W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS. Vol. 2013, p. 11-32.
[107] Seetharaman, A., Saravanan, A. S., Patwa, N., and Mehta, J. (2017). Impact of Bitcoin as a World Currency. Accounting and Finance Research, 6(2), pp. 230–246. https://doi.org/10.5430/afr.v6n2p230

widely used means of payment. They believe that Bitcoin and other cryptocurrencies will become an alternative payment system option in the future.[108]

Moore and Stephen (2015) examined the potential role of digital currency as part of a central bank's foreign asset portfolio. The first of two different scenarios uses a scenario where a portion of the foreign exchange portfolio is invested in bitcoin. The second approach creates artificial shocks using Monte Carlo simulations and examines their impact on the international portfolio. They found that if the Central Bank of Barbados kept a relatively small portion of its portfolio in bitcoin, the volatility that could arise in reserves would not be significantly different from the volatility that would occur when holding major currencies. They stated that as the percentage allocated to bitcoin increases, portfolio volatility will increase, and if valued against the dollar, it will provide a return to the bank.[109]

Folkinstein et al. (2015) tried to explain how Bitcoin works as a cost-effective money transfer system and why it can serve as a disruptive financial technology with examples from the existing system. As a result, Bitcoin, etc. offers better features than the existing system. They believe that formations can change the system.[110]

Glaser et al. (2014) investigated whether Bitcoin is being used as a currency or an alternative investment vehicle, and as a result, they noticed that especially new users retain Bitcoin as a speculative investing tool in their wallets and do not use it to provide goods and services. The study used an ARCH model with a dataset of daily values from January 1, 2011 to October 8, 2013.

Baur, Hong, and Lee (2015) attempted to answer whether Bitcoin is a currency or a financial asset by analyzing users and comparing traditional financial assets. As a result of the

[108] Luther, W., and White, L. (2014). Can bitcoin become a major currency?. George Mason University, pp. 14-17 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446604

[109] Moore, W., and Stephen, J. (2015). Should Cryptocurrencies Be Included in the Portfolio of International Reserves Held by the Central Bank of Barbados? Central Bank of Barbados WP/15/16. Central Bank of Barbados. https://doi.org/10.2139/ssrn.2775396

[110] Folkinshteyn, D., Lennon, M. M., and Reilly, T. (2015). The Bitcoin Mirage: An Oasis of Financial Remittance. Journal of Strategic and International Studies, Forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2601621

research, few users seem to use bitcoin as a medium of exchange, which shows that it is more for investment purposes.[111]

Briere et al. (2015) tested portfolio diversification by including Bitcoin in a portfolio built using traditional assets and alternative investments in their study using weekly data from 2010 to 2013. Bitcoin has a low correlation with traditional financial assets. It has been stated that even a small amount of bitcoins included in a well-diversified portfolio will significantly increase its risk and reward characteristics, which can bring high returns.[112]

Van Wijk (2013) investigated the impact of stock markets, exchange rates and oil prices on Bitcoin and concluded that many financial indicators, including the Dow Jones index, the euro-dollar exchange rate, and the price of WTI crude oil, have a significant impact on the cost of bitcoin. Bitcoin in the long run. The Dow Jones also has a significant impact on bitcoin in the short term.[113]

Strokal (2018) evaluated Bitcoin in terms of the characteristics of money. Studying Bitcoin from an Austrian school perspective, he analyzed the consistency of Bitcoin as a medium of exchange with Mises's regression theorem. As a result, he stated that Bitcoin can compete with traditional currencies in terms of being a medium of exchange, and this depends on the prevalence of Bitcoin use in free markets and time.[114]

Beck and Elbeck (2015) looked for an answer to the question of whether Bitcoin is an investment vehicle or a speculative instrument by assessing volatility with daily data from Bitcoin and the S&P 500 Index. The results show that Bitcoin prices are about 26 times more volatile than

[111] Baur, D. G., Hong, K. J., and Lee, A. D. (2016). Bitcoin – Currency or Asset? 2016 Financial Institutions, Regulation & Corporate Governance (FIRCG) Conference. https://papers.ssrn.com/abstract=2736020

[112] Brière, M., Oosterlinck, K., and Szafarz, A. (2015). Virtual currency, tangible return: Portfolio diversification with bitcoin. Journal of Asset Management, 16(6), p. 365–373. Palgrave Macmillan. https://doi.org/10.1057/jam.2015.5

[113] Van Wijk, D. (2013). What can be expected from the Bitcoin? Erasmus Universiteit Rotterdam. Master's Thesis. thesis.eur.nl. https://thesis.eur.nl/pub/14100/Final-version-Thesis-Dennis-van-Wijk.pdf

[114] Stroukal, D. (2018). Can Bitcoin Become Money? Its Money Functions And The Regression Theorem. International Journal of Business and Management, 6(1), pp. 36–53. https://ideas.repec.org/a/sek/jijobm/v6y2018i1p36-53.html

Bitcoin prices. stocks, with bitcoin being a speculative instrument run by buyers and sellers. However, if the use of bitcoin becomes widespread, its volatility is expected to decrease.[115]

7. INTERNATIONAL EXPERIENCE: HOW CRYPTOCURRENCIES ARE REGULATED IN DIFFERENT COUNTRIES

Although it is thought that cryptocurrencies do not pose a great risk to financial stability and monetary policy globally, in terms of their location and market size, it is seen that the developments are followed closely. At the same time, discussions about regulatory studies in the use of cryptocurrencies continue. The fact that cryptocurrencies have an anonymous structure, are not dependent on any central authority and can be easily used in international transfers shows that international studies can be carried out on the Laundering of Proceeds of Crime and Financing of Terrorism. With the high volatility of cryptocurrencies, the fact that crypto currency trading platforms are not subject to any control is considered to be one of the important risks. While the central banks of various countries such as Canada, England, China, Russia, Sweden, Denmark and Iran continue their studies on crypto/digital currencies, studies are also continuing on the compatibility of technology with its possible effects on the financial system and macroeconomics.

However, a study that covers all legal regulations in any country has not yet been put forward. A report was published by The Federal Bureau of Investigation in 2012 – before Bitcoin gained in value and fame after its creation. In the report, it has been evaluated that it will not be possible to observe and detect any suspicious activity that will occur because it is not managed by a central authority, considering that its features may cause difficulties in the economy. For this reason, it has been evaluated that it can be used in illegal activities.[116]

In the Virtual Currencies: Key Definitions and Potential AML/CTF Risks report published by The Financial Action Task Force in 2014, it was stated that since cryptocurrencies can be

[115] Beck, R., and Müller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers. 50th Hawaii International Conference on System Sciences, pp. 5390–5399. http://hdl.handle.net/10125/41815

[116] FBI. (2012). Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. Washington, D.C: Federal Bureau of Investigation. https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

substituted for fiat currencies, they can be used for money laundering and therefore should be followed.

Lagarde (2017), former head of the International Monetary Fund (IMF), stated that cryptocurrencies have risks for the economy, so it will be important to follow up and various regulations can be applied if necessary. Legarde thinks that by evaluating how crypto money technology is, regulations can be made in the future where central banks can use this technology.[117] Christoph N. Dellingshausen (2011), Vice President of the German Digital Economy Association, thinks that crypto/digital currencies such as Bitcoin should enact a law stating that they have responsibilities to protect their citizens and society. Dellingshausen emphasizes the importance of cryptocurrency regulation for the safety and well-being of consumers, as well as for the interests of merchants and online merchants. In addition, it is thought that one of the most important reasons for the regulation of Bitcoin and crypto money is to try to prevent illegal practices such as drug activity.

If no regulation is applied, some problems may arise in public institutions and organizations due to the lack of legal responsibility in bankruptcy or similar cases.[118] Cryptocurrencies may differ from country to country when considered in terms of regulation. While some countries publish reports that there are risks about cryptocurrencies, some countries argue that there is no legal regulation, that it is not recognized as money and cannot be used as a financial instrument. Since cryptocurrencies are not subject to any regulation and do not have any central authority, there are legal gaps. Other problematic areas with regulation and supervision stem from the decentralized nature of cryptocurrencies, issues with money laundering and taxation. Although some countries have studies on completely banning cryptocurrencies, some countries also highlight the option of controlling them. In terms of the development and future use of cryptocurrencies, each country can act with a global level of cooperation by working on its own economic, financial and legal system. In the Table below are the countries that have issued or are

[117] Lagarde, C. (2017). Central Banking and Fintech—A Brave New World? International Monetary Fund Speech. https://www.imf.org/en/News/Articles/2017/09/28/sp092917-centralbanking-and-fintech-a-brave-new-world

[118] Brito, J. and Castillo, A. M. (2016). Bitcoin: a primer for policymakers. Mercatus Center, George Mason University. https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf

preparing to issue their own cryptocurrencies nationally or regionally. When the table is examined, it can be interpreted that these countries are predominantly underdeveloped countries.

Table . Countries with National or Regional Cryptocurrencies

Anguilla
Marshall Islands
Antigua and Barbuda
Montserrat
China
Saint Kitts and Nevis
Dominic
St. Lucia
Grenada
Saint Vincent and the Grenadines
Ireland
Venezuela

While the debates on whether to use cryptocurrencies as a currency or an investment tool continue, the issue of taxation for countries is also on the agenda. While Israel is working on taxing cryptocurrencies as an asset, Bulgaria also applies taxation as a financial asset. Denmark, Spain and Argentina are working to regulate cryptocurrencies as income taxable. In the United Kingdom, work is underway to implement a similar regulation. The UK requires companies to pay corporate tax and individuals to pay capital gains tax for cryptocurrencies. Unlike these countries, Switzerland treats cryptocurrencies as a foreign currency and carries out taxation studies. Along with the subject of taxation, countries also have some studies with the idea that cryptocurrencies are used in money laundering or terrorist activities. Countries like Australia and Canada have expanded their organized crime laws to include money laundering, counter-terrorism and cryptocurrency markets.[119]

[119] The Law Library Congress (2018). Regulation of Cryptocurrency Around the World. International Telecommunications Policy Review.
https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

Table . Countries Applying Taxes and Laws to Cryptocurrencies

Tax Law Practice		Money Laundering and Anti-Terrorism Laws		Both
Argentina	Poland	Cayman Islands	Jersey	Australia
Austria	Russia	Latvia	Luxembourg	Denmark
Bulgaria	Slovakia	Estonia	Liechtenstein	Switzerland
Finland	South Africa	Costa Rica	South Korea	Canada
Israel	Romania	Czech Republic	Singapore	Japan
Iceland	Spain	Gibraltar		
Italy	Sweden	Isle of Man		
Norway	United Kingdom	Hong Kong		

Some countries around the world have banned investing and dealing with cryptocurrencies. Countries such as Algeria, Bolivia, Morocco, Nepal, Pakistan, and Vietnam have banned all activities involving cryptocurrencies. Countries such as Qatar, Bahrain, Bangladesh, Iran, Thailand, Lithuania, Lesotho, China and Colombia, on the other hand, did not both liberalize and prohibit transactions by restricting their citizens' local transactions involving cryptocurrencies.[120]

Table . Countries Banning Cryptocurrencies

Absolutely Forbidden	Partially Forbidden	
Bolivia	Bahrain	Lithuania
Egypt	Chinese	Macau
Algeria	Bangladesh	Oman
Iraq	Colombia	Train
Morocco	Dominican Republic	Taiwan
Pakistan	Indonesia	Saudi Arabia
United Arab Emirates	Iranian	Thailand
Nepal	Lesotho	
Vietnamese	Kuwait	

[120] The Law Library Congress (2018). Regulation of Cryptocurrency Around the World. International Telecommunications Policy Review.
https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

7.1 China

China is one of the countries where Bitcoin mining is done the most.[121] Accordingly, it is thought that any regulation to be made in China will greatly affect investors and users of crypto money. In 2017, seven public institutions working under the Chinese government jointly published a statement. The Bank of China (PBOC), China Cyber Administration (CAC), Ministry of Industry and Information Technology (MIIT), Industry and Trade State Administration (SAIC), China Banking Regulatory Commission (CBRC), China Securities Regulatory Commission (CSRC), and China According to a joint statement released by the Insurance Regulatory Commission (CIRC), cryptocurrencies are considered to be illegal assets. The announcement also warned that cryptocurrencies are not supported by any monetary authority, and therefore should not be used in circulation, and it is prohibited.[122]

The People's Bank of China (PBOC), which has been working for a long time, is conducting research on the legal status of cryptocurrencies. Former Bank President Zhou Xiaochuan considers that Chinese regulators are not yet viable to use cryptocurrencies such as Bitcoin for retail payments. Zhou Xiaochuan stated that the Chinese banking system is not yet able to accept cryptocurrencies and provide related services. Although China bans cryptocurrencies, it has decided to issue its national cryptocurrency. The People's Bank of China (POBC) continues to work on a cryptocurrency that can perform the same function as fiat currencies.[123]

7.2 Unıted States of America

Since the United States of America has the largest economic size in the world, has the most crypto money in the world and is the world leader in the volume of cryptocurrencies, any regulation regarding Bitcoin or cryptocurrencies affects the whole world and other countries too. attracts attention. Despite the high interest in Bitcoin and cryptocurrencies in the United States, it is

[121] Tuwiner, J. (2019). Bitcoin Mining in China. https://www.buybitcoinworldwide.com/mining/china/

[122] PBOC (2017). Announcement of the China Insurance Regulatory Commission. The China Banking Regulatory Commission. http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html

[123] Lagerfeld., F. (2019). China Appoints MU Changchun as New Digital Currency Head. https://www.nextrankers.com/china-appoints-mu-changchun-as-newdigital-currencyhead/

thought that a consensus has not been reached. The Chicago Central Bank, which is affiliated with the United States Federal Reserve (FED), published a report on Bitcoin in 2013. In the report prepared by Expert Economist Françoiş Velde, it is stated that when Bitcoin and similar crypto money transactions are followed from 2009 to 2013, Bitcoin and crypto money will not yet function as a medium of exchange, excluding illegal activities.

In the report, Bitcoin and altcoins are considered as a speculative investment opportunity. The United States Government Accountability Office published a report on Bitcoin and cryptocurrencies in 2014. In the report, although there is no legal definition for cryptocurrencies, a digital representation of a value that is not recognized by the state has been defined. According to the report, it has been stated that cryptocurrencies can fulfill the functions of fiat money as a unit of account and a medium of exchange, but regulation can be made because it is not widespread and not yet acceptable.[124]

Considering the report published by The Financial Crimes Enforcement Network of the United States Department of the Treasury in 2013, The International Revenue Service accepts Bitcoin as a real currency, although it does not have any legal status. In addition, the IRS stated that besides being accepted as a real currency, Bitcoin is also convertible and exchangeable for real money.[125]

A 2014 report by The U.S. Securities and Exchange Commission stated that any investment in securities in the United States, whether made in US dollars or crypto/virtual currency, remains subject to SEC jurisdiction. However, in the report, it was also emphasized that caution should be exercised by warning against the possibility of fraud. In the United States, for the first time in 2015, a final decision was made regarding Bitcoin from cryptocurrencies. According to the law enacted in the United States state of New York, Bitcoin can be bought and held as an asset.[126]

---

[124] United States Government Accountability Office (2014) Virtual Currencies. Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate.
https://www.gao.gov/assets/670/663678.pdf

[125] The International Revenue Service (2014). Notice 2014-21. https://www.irs.gov/pub/irs-drop/n-14-21.pdf

[126] Popper, N. (2015). Bitcoin Exchange Receives First License in New York State
https://www.nytimes.com/2015/05/08/business/dealbook/bitcoin-exchangereceives-first-license-in-new-york-state.html?_r=2

Former Chairman of the United States Federal Reserve (FED), Janet Yellen, stated in an assessment she made in 2017 that Bitcoin is a speculative asset and that it has not yet been able to base it on a legal basis. In 2018, Morgan Stanley, one of the investment banks of the United States, published a report on Bitcoin and cryptocurrencies. In the report, it is stated that there may be a regulation regarding Bitcoin in the future, but there is no consensus on this issue yet. In addition, according to the report, it was evaluated that the regulations made about Bitcoin, cryptocurrencies or blockchain may cause a decrease in the interest in this technology.

Hester Peirce, a member of the United States Securities and Exchange Commission, stated in a statement in 2019 that digital assets are important and can be used as money in the future with the development of technology. Pierce thinks that the United States needs to act a little faster on regulation and this makes the United States less competitive. Pierce evaluated that the SEC is also working on this issue and that they should act more quickly in regulating. There seems to be no consensus for cryptocurrencies in the United States yet. It is thought that the United States, which is described as the world's largest economy and has the world's largest stock market, will attract the attention of the whole world in case of any regulation regarding cryptocurrencies. According to the opinions of the United States public institutions and high-level officials, it can be interpreted that cryptocurrencies are expected to be defined first and then to act with regulations to be created within the framework of consensus.[127]

7.3 Russıa

The Russian Ministry of Technology and Mass Media announced that mining has become legal by making important regulations regarding cryptocurrencies in 2018. With this regulation, miners can continue their activities under the name of industrial mining if they meet the energy consumption requirements and register with the tax office. It has also been announced that these miners will be exempt from tax for two years.[128]

[127] Zheng, S. (2019). SEC Commissioner Hester Peirce says digital assets could one day be the money of the internet. https://finance.yahoo.com/news/seccommissioner-hester-peirce-says-182020019.html

[128] RBC (2018). How cryptocurrencies and ICO's will be regulated in Russia. https://www.rbc.ru/finances/20/03/2018/5ab125e69a79474518a5c2a1

The Ministry of Finance of Russia introduced a draft law on digital financial assets in 2018. According to the law, mining was defined as the activity carried out with the aim of producing cryptocurrency. In addition, it has been decided by the law that if the electricity consumption spent during mining activity exceeds the level determined by the state for three consecutive months, it will be considered as an entrepreneurial activity subject to taxation. While various regulations regarding cryptocurrencies are being made in Russia, a definite decision has not been made yet. Russia, which cannot decide on how to apply taxation to crypto money investors, seems to have not yet reached a consensus on the rights of these investors.

7.4 European Unıon

Mario Draghi, President of the European Central Bank (ECB), made an assessment on Bitcoin and cryptocurrencies in 2018. Draghi thinks that attention should be paid, stating that he considers Bitcoin and cryptocurrencies to be very risky assets due to high volatility. At the same time, Draghi explained that cryptocurrencies do not have a certain control yet, and studies are ongoing for a control mechanism.[129]

The European Commission announced an action plan in 2018. In the action plan it announced, the Commission made evaluations about how it can benefit from innovations that can be used in financial services such as blockchain. In the action plan, it was decided to establish the EU Blockchain Observatory and Forum, which will report on the challenges and opportunities of cryptocurrencies and work on a comprehensive strategy for the use of blockchain to cover all sectors of the economy. Deutsche Bundesbank published a statement about Bitcoin in 2018. Bundesbank payments expert Dirk Schrade states that Bitcoin is not a currency that can be used in any virtual environment. Schrade considers that Bitcoin is not yet part of the monetary system, as it cannot fulfill the functions of a currency.[130] A decree that came into force in France in 2018 allowed the use of blockchain technology for financial instruments.[131]

---

[129] ECB (2018). European Parliament plenary debate on the ECB Annual Report for 2016. Speeches.
https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180205.en.html

[130] Bundesbank (2018). Bitcoin is not a virtual currency.
https://www.bundesbank.de/en/tasks/topics/-bitcoin-is-not-a-virtual-currency--667600

[131] Legifrance (2018) Regarding the Use of a Shared Electronic Registration Method for the Representation and Conveyance of Financial Instruments. Other Laws and Regulations.
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908

In addition, legislative and executive institutions affiliated to the parliament in the country are actively researching how to best regulate cryptocurrencies. The European Union Blockchain Observatory and Forum, established by the European Parliament with the action plan of the European Commission, published the Legal And Regulatory Framework Of Blockchains And Smart Contracts report in 2019. The report emphasized that as the use of blockchain technology becomes more widespread, regulatory processes will become more difficult. However, in the report, it is evaluated that these difficulties are natural and that the change process will take place in this way. Studies on the use and regulation of blockchain technology continue. It is thought that these studies may also affect cryptocurrencies. When the studies of the European Union and its countries are examined, it can be evaluated that they attach importance to cryptocurrencies and follow them, but it is seen that the studies on the blockchain are more concentrated. This may lead to the interpretation that the European Union attaches more importance to the blockchain, the technology used by cryptocurrencies, and cares more for the future.[132]

7.5 South Korea

South Korea is one of the countries that act boldly about cryptocurrencies. Choe Heung, Chairman of the South Korean Financial Supervisory Authority, announced that the government will support the trading of cryptocurrencies and encourage financial institutions to facilitate the trading of cryptocurrencies. The South Korean government passed a law in 2018 allowing transactions with cryptocurrencies from real bank accounts. The government, which does not allow any crypto currency transactions anonymously, has also prevented foreigners from making transactions with crypto money in the country. This allows for state-controlled transactions with cryptocurrencies within the country for South Korean citizens.[133]

7.6 Japan

Japan Financial Services Agency has been working since 2018 to make an important regulation in the crypto money market. According to the draft law that the agency is considering to submit, it plans to protect the people who use these assets by making it mandatory to display fiat money in

[132] European Commission (2018). European Commission launches the EU Blockchain Observatory and Forum. Press Release.
https://europa.eu/rapid/press-release_IP-18-521_en.htm

[133] Zheng (2018). Choi Heung-Sik, Financial Supervisory Commissioner.
http://www.yonhapnews.co.kr/bulletin/2018/02/20/0200000000akr20180220100700002.html

exchange for digital assets on cryptocurrency exchanges. The Financial Services Agency is also working to make the public offering of cryptocurrencies legal.

7.7 Singapore

One of the most attractive countries for setting up fintech and blockchain businesses. The country is striving to become a smart financial center. The third largest ICO market, featuring major crypto exchanges such as US-based Coinbase, GDAX and Gemini, hosts the world's largest forum, the Singapore Fintech Festival. The development of the fintech ecosystem is supported through various tools, incl. a working group for the development of regulation Fintech and Innovation Group, a fintech laboratory Looking Glass, the world's largest crypto hub, was created. The Monetary Authority of Singapore (MAS) regulates cryptocurrency transactions if they are products that fall under the Securities and Futures Act. In this case, issuers must register the issue of tokens - securities (prospectus), and intermediaries and trade organizers must obtain appropriate licenses. At the same time, these requirements are not applied to crypto-exchanges if they do not accept tokens for trading - securities. The regulator's position is fixed in the ICO guide.[134] In the event of a violation, the regulator, as a rule, issues a warning to the ICO organizer. In response to the warning, some ICO organizers simply return funds received from Singapore during the ICO. The sale and exchange of cryptocurrencies for a certain monetary reward is recognized as a taxable provision of services.[135] The exchange of cryptocurrencies among themselves is not regulated and does not fall under the AML procedures, which at the same time does not apply to the procedures for transferring to fiat currencies.

7.8 Switzerland

One of the most attractive jurisdictions for companies operating in the blockchain field, which is ensured by progressive legislation, friendly regulation in relation to the crypto industry, tax regime, and a developed banking sector. Within the canton of Zug, the necessary ecosystem for the blockchain is being formed - the Crypto Valley (Crypto Valley Association). In general,

---

[134] Monetary Authority of Singapore,
http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%2014%20Nov%202017.pdf

[135] Payment Services Bill in November 2017,
https://www.bakermckenzie.com/en/insight/publications/2018/01/the-proposed-payment-services-bill

the legislation is based on the principle of technological neutrality. Cryptocurrencies do not have an official legal status. They are considered as assets in accordance with the report of the Swiss Federal Council (clause 2.2.1) and are reflected accordingly in accounting documents, except for the purposes of applying VAT - they are equated to currencies.[136]

The use of cryptocurrencies does not require licenses. When carrying out activities on a commercial basis, compliance with AML / CFT requirements is required. For the legalization (laundering) of money obtained by criminal means with the help of cryptocurrencies, the application of the norms of the Criminal Code (Swiss Criminal Code, 305bis SCC) is provided.
Crypto exchanges must become a member of a self-regulatory organization or obtain a license of a controlled financial intermediary from FINMA (DSFI) before starting operations. In some cases, a banking license may be required (for example, storing / managing clients' money).
In February 2018, the Swiss Financial Market Supervision Authority (FINMA) published recommendations for the ICO, under which it identified the following types of tokens: payment tokens, utility tokens, asset tokens, hybrid tokens.[137]

In the event that fundraising within the ICO exceeds 1 million francs, it is necessary to obtain licenses for fundraising. As a general rule, fundraising activities do not fall under the regulation of financial markets if the company does not have obligations to return the borrowed funds, has not issued means of payment, and there is no secondary circulation market.

[136] http://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf
[137] https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

CONCLUSION

As a result of many events of the 21st century, the concept of globalization has emerged. The technologies that appeared along with the development of this process have greatly influenced human life. The fact that technology is present in all aspects of human life and provides convenience has highlighted the idea of the need for more reliable money that could be used in the digital environment instead of paper money. From smartphones to tablets, from robots to spacecraft, from smartwatches to smart home assistants, the growing trust in technology, which continues to evolve at unattainable rates in many areas, has led to doubts about a monetary system based on trust. ... Some recent economic and political events have shaken people's confidence in the monetary system, and authorities have begun to question it. In the course of discussions about whether to use a new monetary system, a cryptological monetary system called Bitcoin has emerged that can be used in a digital environment. Bitcoin based on blockchain technology can be seen as the latest example of a technology that is in perpetual change and development, penetrating all areas of our life. In monetary systems, trust is the most important underlying phenomenon. If people don't trust the currencies they use, they won't trust the economy's money management system. This can encourage people to turn to alternative currencies or instruments they trust more. Whether it's paper money or cryptocurrencies, it's important to gain public trust. The global financial crisis in 2008 eroded confidence in the authorities and led to criticism of policies. In this environment, prevailing during the crisis, economic criticism intensified, and discussions began on the creation of an alternative currency to reserve currencies. Cryptocurrencies that have arisen as a result of addressing the problems of the current monetary system have led to requests for a new monetary system with discussions if it can solve these problems. One of the most important reasons for the emergence of cryptocurrencies and bitcoins is trust. Cryptocurrencies have many advantages when considering the current monetary system. Cryptocurrencies have much lower transaction costs. Cryptocurrencies have advantages such as faster and easier transaction execution compared to fiat currencies. If you add a public trust mechanism to these functions, you might think that cryptocurrencies could be used instead of fiat currencies in the future. However, one of the most important features of cryptocurrencies is that they do not have a centralized structure. While cryptocurrencies have these functions and can perform them, their decentralized function is questionable on the other side. The biggest reason for the emergence of cryptocurrencies is that they do not have a centralized structure. A controversial situation will arise due to the use of

cryptocurrencies, which are believed to be offered centrally, contrary to its structure. If cryptocurrencies continue to exist in the market in a decentralized manner, they may be subject to any regulation by central authorities that they consider to be a threat. Central authorities who believe that cryptocurrencies do not pose a threat can enact appropriate regulations. However, when cryptocurrencies gain the trust of society and become a tool that is used effectively, it can be interpreted that the traditional monetary system will eventually be replaced.

With the decentralized use of cryptocurrencies, the control of the central authorities, especially the central bank, will disappear from the market. This is not what the central authorities and states want. Consequently, the arrival of cryptocurrencies in such a position in the future will force states to take even more prohibitive measures. In the event that cryptocurrencies are offered by central banks, there may be some changes to the policy. Leveraging existing crypto / digital currency policies can lead to policy inefficiencies and disruptions. Monetary policy needs to be reviewed and new policies defined. While it is believed that monetary policy of central banks will be more successfully implemented through the supply of crypto / digital money, the purpose of the emergence of cryptocurrencies is not to have a central authority. The issuance of a cryptocurrency by a central authority can be thought of as an electronic or digital version of existing money. However, central banks will create their own crypto money to keep up with this technology. However, society will believe that the money used in the digital environment is reliable and efficient. Over time, this situation can increase the confidence in cryptocurrencies that are emerging decentralized, and can lead to the deformation or collapse of the existing monetary system in the future.

BIBLIOGRAPHY

Ahn, J., Khandelwal, A. K., and Wei, S.-J. (2011). The role of intermediaries in facilitating trade. Journal of International Economics, 84(1), pp. 73-85.

Akins, B. W., Chapman, J. L., and Gordon, J. M. (2014). A whole new world: Income tax considerations of the Bitcoin economy. Pitt. Tax Rev., 12, pp. 25-58.

Akolkar, B. and Sharma, S. (2021). Tether (USDT) Conspiracy Tosses Again As We Arrive at The D-Day of January 15, https://coingape.com/tether-usdt-conspiracy-tosses-again-as-we-arrive-at-the-d-day-of-january-15/

Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain (2. Vol.). O'Reilly. https://www.bitcoinbook.info/

Bacon, J., Michels, D. J., Millard, C. and Singh, J. (2017). Blockchain Demystified. Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017

Barski, C. and Wilmer, C. (2015). Bitcoin For The Befuddled, San Francisco, p.112.

Baur, D. G., Hong, K. J., and Lee, A. D. (2016). Bitcoin – Currency or Asset? 2016 Financial Institutions, Regulation & Corporate Governance (FIRCG) Conference. https://papers.ssrn.com/abstract=2736020

Baur, D., Hong, K., and Lee, A. (2018). Bitcoin: Medium of exchange or speculative assets?, Journal of International Financial Markets, Institutions and Money. № 54. pp. 177-189.

Beck, R., and Müller-Bloch, C. (2017). Blockchain as Radical Innovation: A Framework for Engaging with Distributed Ledgers. 50th Hawaii International Conference on System Sciences, pp. 5390–5399. http://hdl.handle.net/10125/41815

Benjamin, B. (2016). 2016 State of the Dark Web, Akamai, Threat Advisory, p.6

Bill Gates: I would short bitcoin if I could. CNBC. 07.05.2018: https://www.cnbc.com/2018/05/07/bill-gates-i-would-short-bitcoin-if-i-could.html.

Bitcoin and Money Laundering, Developments In Banking Law. Boston University, 2016-2017, https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjE4MGrwdnYAhVREVAKHScGAtsQFggnMAA&url=https%3A%2F%2Fwww.bu.edu%2Frbfl%2Ffiles%2F2017%2F03%2FDA-13.pdf&usg=AOvVaw1cHZOX80URnsw9maXFlCtQ

Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), pp. 213-238.

Brière, M., Oosterlinck, K., and Szafarz, A. (2015). Virtual currency, tangible return: Portfolio diversification with bitcoin. Journal of Asset Management, 16(6), p. 365–373. Palgrave Macmillan. https://doi.org/10.1057/jam.2015.5

Brito, J. and Castillo, A. M. (2016). **Bitcoin: a primer for policymakers**. Mercatus Center, George Mason University. https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf

Bundesbank (2018). **Bitcoin is not a virtual currency**. https://www.bundesbank.de/en/tasks/topics/-bitcoin-is-not-a-virtual-currency--667600

Burkart, M., and Ellingsen, T. (2004). In-kind finance: A theory of trade credit. American Economic Review, 94(3), pp. 569-590.

Buterin, V. (2015). Visions, Part 1: The Value of Blockchain Technology, Ethereum Blog, https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/.

Castells, M. (2001). The Internet Galaxy. Oxford University Press

Chen, C. Y., Härdle, W. K., Hou, A. J., and Wang, W. (2018). Pricing Cryptocurrency options: the case of CRIX and Bitcoin.

China Coin No More: Bitcoin Mining Shifting to Sweden and Norway, 27.12.2020, https://u.today/chinacoin-no-more-bitcoin-mining-shifting-to-sweden-and-norway

Chohan, U. (2017). Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability

Ciaian, P., and Rajcaniova, M. (2016). The digital agenda of virtual currencies: Can BitCoin become a global currency?. Information Systems and e-Business Management, 14(4), pp. 883-919.

CoinDesk, (2018). https://www.coindesk.com/bitmain-by-the-numbers-an-inside-look-at-a-bitcoin-mining-empire

CoinMarketCap, (2019). Bitcoin price, charts, market cap, and other metrics, https://coinmarketcap.com/currencies/bitcoin/

Conte de Leon, D., Stalick, A. Q., and Sheldon, F. T. (2017). Blockchain: properties and misconceptions. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3), pp.286–300

Corbet, S., Larkin, C. J., Lucey, B. M., and Yarovaya, L. (2018). Kodakcoin: A Blockchain Revolution or Exploiting a Potential Cryptocurrency Bubble?

Cortese, A. (2016). Blockchain technology ushers in the Internet of Value, Cisco Feature Story, https://newsroom.cisco.com/feature-content?articleId=1741667

Costelloe, K. (2017). Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says: https://www.bloomberg.com/news/articles/2017-11-29/bitcoin-ought-to-be-outlawed-nobel-prize-winner-stiglitz-says-jal10hxd

Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018, https://powercompare.co.uk/bitcoin-mining-electricity-map/

Darlington III, J. K. (2014). The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency Through Benefit Analysis.

De Filippi, P., and Wright, A. (2018). Blockchain and the Law: The Rule of Code, Harvard University Press, p. 663

de Leon, D. C. et. al. (2017). Blockchain: properties and misconceptions", Asia Pacific Journal of Innovation and Entrepreneurship, Vol. 11, Issue. 3, pp. 286–300

Double Spending Explained, https://academy.binance.com/en/articles/double-spending-explained

ECB (2018). **European Parliament plenary debate on the ECB Annual Report for 2016.** Speeches.

Ethereum, Licensing - Ethereum/wiki, GitHub, (2019), https://github.com/ethereum/wiki/wiki/Licensing Development - Bitcoin, Bitcoin.org, (2019), https://bitcoin.org/en/development#code-review

European Commission (2018). **European Commission launches the EU Blockchain Observatory and Forum.** Press Release. https://europa.eu/rapid/press-release_IP-18-521_en.htm

European Parliament, (2018). Cryptocurrencies and Blockchain; Legal context and implications for financial crime, money laundering and tax evasion, July, p.33

European Parliament, Virtual Currencies and Central Banks Monetary Policy: Challenges Ahead, p.13.

FBI. (2012). **Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.** Washington, D.C: Federal Bureau of Investigation. https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Finck, M. (2018). Blockchain Regulation and Governance in Europe. Cambridge: Cambridge University Press. https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/A722E0522BC6C5300AA0813340BD6C04#

Folkinshteyn, D., Lennon, M. M., and Reilly, T. (2015). The Bitcoin Mirage: An Oasis of Financial Remittance. Journal of Strategic and International Studies, Forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2601621

Franco, P. (2015). Understanding Bitcoin. UK: John Wiley and Sons Ltd

Frankenfield, A. (2019). Tether (USDT), https://www.investopedia.com/terms/t/tether-usdt.asp#:~:text=Tether%20is%20a%20blockchain%2Dbased,trade%20under%20the%20USDT%20symbol

Frederik, A., Ghassan, O. K., Avikarsha, M. and Franck, Y. (2015). Ripple: Overview and Outlook, pp.2-3.

Gandal, N. and Halaburda, H. (2014). Competition in the Cryptocurrency Market. https://www.econstor.eu/bitstream/10419/103022/1/791932281.pdf

Halaburda, H. and Sarvary, M. (2016). Beyond Bitcoin The Economics of Digital Currencies, New York, pp.104-108

Harwick, C. (2016). Cryptocurrency and the Problem of Intermediation. http://www.independent.org/pdf/tir/tir_20_04_05_harwick.pdf

Hayes, A. S. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. Telematics and Informatics, 34(7), pp. 1308-1321.

Heid, A. (2013). Analysis of the Cryptocurrency Marketplace. Retrieved February, 15

Hendrickson, J. R., Hogan, T. L., and Luther, W. J. (2016). The political economy of bitcoin. Economic Inquiry, 54(2), pp. 925-939.

Hepp, A. (2016). Pioneer communities: collective actors in deep mediatisation, Media, Culture and Society, Vol. 38, Issue. 6, pp. 918–33

Herrera, A. I. and Hunter, T. (2018). Oil as Currency: Venezuela's Petro, a New 'Oil Pattern'?. SSRN Electronic Journal. 10.2139/ssrn.3291272.

http://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf

https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180205.en.html

https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

Hu, J., Luo, Q., and Zhang, J. (2020). The Fluctuations of Bitcoin Price during the Hacks. 3. pp. 10-20. 10.33422/ijarme.v3i1.278.

Javarone, M. A., and Wright, C. S. (2018). From Bitcoin to Bitcoin Cash: a network analysis. 1804.02350. pp. 1-5.

Julianne, H. Josh, O. and John, S. (2018). Ethereum vs. Bitcoin, California, p.3.

Karishnan, H., Saketh, S., and Vaibhav, V. T. (2015). Cryptocurrency Mining – Transition to Cloud, International Journal of Advanced Computer Science and Applications, Vol. 6, No. 9, India, p.115

Karishnan, S. et. al. (2016). Cryptocurrency Mining – Transition to Cloud, International Journal of Advanced Computer Science and Applications, p.115.

Kochergin, D.A. (2020). Pokrovskaya N.V. International experience in taxation of cryptoassets, Economic Journal of the Higher School of Economics, no. 24 (1). S. 53-84

Kostakis, V., and Giotitsas, C. (2014). The (A) political economy of Bitcoin. TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society, 12(2), pp. 431-440.

Kroll, J. A., Davey, I. C., and Felten, E. W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS. Vol. 2013, p. 11-32.

Lagarde, C. (2017). **Central Banking and Fintech—A Brave New World?** International Monetary Fund Speech. https://www.imf.org/en/News/Articles/2017/09/28/sp092917-centralbanking-and-fintech-a-brave-new-world

Lagerfeld., F. (2019). **China Appoints MU Changchun as New Digital Currency Head.** https://www.nextrankers.com/china-appoints-mu-changchun-as-newdigital-currencyhead/

Legifrance (2018) Regarding the Use of a Shared Electronic Registration Method for the Representation and Conveyance of Financial Instruments. Other Laws and Regulations. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908

Li, X., and Wang, C. A. (2017). The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. Decision Support Systems, 95, pp. 49-60.

Limer, E. (2013). The World's Most Powerful Computer Network Is Being Wasted on Bitcoin, https://gizmodo.com/the-worlds-most-powerful-computer-network-is-being-was-504503726,

Lischke, M., and Fabian, B. (2016). Analyzing the bitcoin network: The first four years. Future Internet, 8(1), pp. 7-47.

Luther, W., and White, L. (2014). Can bitcoin become a major currency?. George Mason University, pp. 14-17 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2446604

Monetary Authority of Singapore, http://www.mas.gov.sg/

Moore, W., and Stephen, J. (2015). Should Cryptocurrencies Be Included in the Portfolio of International Reserves Held by the Central Bank of Barbados? Central Bank of Barbados WP/15/16. Central Bank of Barbados. https://doi.org/10.2139/ssrn.2775396

Morisse, M. (2015). Cryptocurrencies and bitcoin: Charting the research landscape. Twenty-first Americas Conference on Information Systems, Puerto Rico. pp. 1-16.

Mosakova, E.A. (2002). National cryptocurrency as Venezuela's economic development factor in the 21st century, Iberoamérica. no. 1. pp. 160-176.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, p.3.

Nakamoto, S. (2009). Bitcoin open source implementation of P2P currency, Satoshi Nakamoto Institute. https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/3/

Narayanan, A. and Clark, J. (2017). Bitcoin's Academic Pedigree. Communications of the ACM, 60(12), pp.36–45.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. New Jersey: Princeton University Press.

Nian, L. M., and Chuen, D. L. K. (2015). Introduction to Bitcoin. Handbook Of Digital Currency. Elsevier Inc.

Nian, L. M., and Chuen, D. L. K. (2015). Introduction to Bitcoin. Handbook Of Digital Currency. Elsevier Inc.

Nishibe, M. (2016). The Enigma of Money Gold, Central Banknotes and Bitcoin, Japan.

Payment Services Bill in November 2017, https://www.bakermckenzie.com/en/insight/publications/2018/01/the-proposed-payment-services-bill

PBOC (2017). **Announcement of the China Insurance Regulatory Commission**. The China Banking Regulatory Commission. http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html

Popper, N. (2015). **Bitcoin Exchange Receives First License in New York State** https://www.nytimes.com/2015/05/08/business/dealbook/bitcoin-exchangereceives-first-license-in-new-york-state.html?_r=2

Quantum Computers Pose Imminent Threat to Bitcoin Security, http://www.comp.nus.edu.sg/news/news-media/2176-2017-quantum-computers/

RBC (2018). **How cryptocurrencies and ICO's will be regulated in Russia.** https://www.rbc.ru/finances/20/03/2018/5ab125e69a79474518a5c2a1

Rosario, N. M. (2017). What's in a Name? From Bitcoin to Blockchain to Distributed Ledgers, https://www.coindesk.com/whats-in-a-name-from-bitcoin-to-blockchain-to-distributed-ledgers;

Seetharaman, A., Saravanan, A. S., Patwa, N., and Mehta, J. (2017). Impact of Bitcoin as a World Currency. Accounting and Finance Research, 6(2), pp. 230–246. https://doi.org/10.5430/afr.v6n2p230

Seetharaman, A., Saravanan, A., Patwa, N., and Mehta, J. (2017). Impact of Bitcoin as a World Currency. Accounting and Finance Research, 6(2), 230.

Shahzad, S. J. H., Bouri, E., and Lucey, B. (2019). Is Bitcoin a better safe-haven investment than gold and commodities?. International Review of Financial Analysis. In Press.

Shetewy, N., Ait, L. J., and Li, J.-J. (2019). Challenges of the Bitcoin in the Arabic Countries.

Sotiropoulou, A. and Ligot, S. (2019). Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?. European Company and Financial Law Review. 16. 652-676. 10.1515/ecfr-2019-0023.

Sterry, D. R. (2012). Introduction to Bitcoin Mining, A Guide Gamers, Geeks, and Everyone Else, pp.10-14.

Stroukal, D. (2018). Can Bitcoin Become Money? Its Money Functions And The Regression Theorem. International Journal of Business and Management, 6(1), pp. 36–53. https://ideas.repec.org/a/sek/jijobm/v6y2018i1p36-53.html

Tasca, P. (2015). Digital Currencies: Principles, Trends, Opportunities, and Risks. https://faculty.fuqua.duke.edu/~charvey/Teaching/898_2017/Readings/Tasca.pdf

Tasca, P., Hayes, A., and Liu, S. (2018). The evolution of the bitcoin economy: extracting and analyzing the network of payment relationships. The Journal of Risk Finance, 19(2), pp. 94-126.

The International Revenue Service (2014). **Notice 2014-21**. https://www.irs.gov/pub/irs-drop/n-14-21.pdf

The Law Library Congress (2018). **Regulation of Cryptocurrency Around the World.** International Telecommunications Policy Review.

Trademarks, J. (2019). Stiftung Ethereum (Foundation Ethereum) Trademarks, https://trademarks.justia.com/owners/stiftung-ethereum-foundation-ethereum-3479392/

Tuwiner, J. (2019). Bitcoin Mining in China. https://www.buybitcoinworldwide.com/mining/china/

United States Government Accountability Office (2014) **Virtual Currencies.** Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate. https://www.gao.gov/assets/670/663678.pdf

Van Wijk, D. (2013). What can be expected from the Bitcoin? Erasmus Universiteit Rotterdam. Master's Thesis. thesis.eur.nl. https://thesis.eur.nl/pub/14100/Final-version-Thesis-Dennis-van-Wijk.pdf

Vigna, P., & Casey, M. (2016). Cryptocurrency: The future of money.

Vigna, P., & Casey, M. (2016). Cryptocurrency: The future of money.

Virtual Currencies Mining the Possibilities, Allen&Overy, 2015, p.4.

Vitalik Buterin reveals Ethereum at Bitcoin Miami 2014, YouTube, (2014), https://www.youtube.com/watch?v=l9dpjN3Mwps

Vovchenko, G., Tishchenko, N., Epifanova, V., and Gontmacher, B. (2017). Electronic Currency: The Potential Risks to National Security and Methods to Minimize Them. European Research Studies Journal, 20(1), pp. 36-48.

Walch, A. (2017). The Path of the Blockchain Bexicon (and the Law), Review of Banking and Financial Law, Vol. 36, pp. 719–20

What is Ethereum 2.0? (Release, Roadmap, Phases), https://www.benzinga.com/markets/cryptocurrency/20/11/18489382/what-is-ethereum-2-0-release-roadmap-phases

What is Ethereum 2.0? Overview, Features and Price Implications, https://www.diginex.com/insights/what-is-ethereum-2-0-overview-features-and-price-implications/

Wörner, D., Von Bomhard, T., Schreier, Y. P., and Bilgeri, D. (2016). The Bitcoin ecosystem: disruption beyond financial services?. Twenty-Fourth European Conference on Information Systems (ECIS), pp. 1-16.

www.bitcoin.com

Yeoh, P. (2017). Regulatory issues in blockchain technology, Journal of Financial Regulation and Compliance, Vol. 25, Issue. 2, p. 2, doi:10.1108/JFRC-08-2016-0068

Zheng (2018). **Choi Heung-Sik, Financial Supervisory Commissioner**. http://www.yonhapnews.co.kr/bulletin/2018/02/20/0200000000akr20180220100700002.html

Zheng, S. (2019). **SEC Commissioner Hester Peirce says digital assets could one day be the money of the internet.** https://finance.yahoo.com/news/seccommissioner-hester-peirce-says-182020019.html

Zimba, A., Wang, Z., Mulenga, M., and Odongo, N. (2018). Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. Journal of Computer Information Systems. 60. 1-12. 10.1080/08874417.2018.1477076.