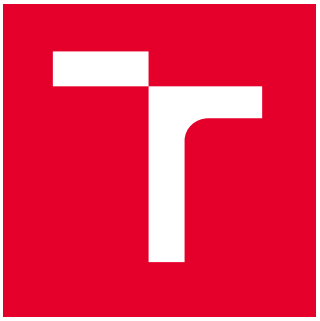

BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES

ÚSTAV JAZYKŮ

CRYPTOCURRENCY – A MODERN KIND OF MONEY

KRYPTOMĚNA – NOVODOBÝ DRUH PENĚZ

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR — **Vojtěch Petrenec**
AUTOR PRÁCE

SUPERVISOR — **Mgr. Jana Jašková, Ph.D.**
VEDOUCÍ PRÁCE

BRNO 2022

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

Bachelor's Thesis

Bachelor's study field **English in Electrical Engineering and Informatics**

Department of Foreign Languages

Student: Vojtěch Petrenec ***ID:*** 208998

Year of study: 3 ***Academic year:*** 2021/22

TITLE OF THESIS:

Cryptocurrency – a modern kind of money

INSTRUCTION:

The aim of the thesis is to describe the concept of digital currency and discuss its properties compared to traditional money.

RECOMMENDED LITERATURE:

Ajiboye, T., Buenaventura, L., Gladstein, A., Liu, L., Lloyd, A., Machado, A., Song, J., & Vránová, A. (2019). The little bitcoin book: Why bitcoin matters for your freedom, finances, and future. 21 Million Books.

Furneaux. N. (2018). Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence. Wiley.

Lee, D., & Deng, R. (Eds.) (2018). Handbook of blockchain, digital finance, and inclusion (Volume 1, Cryptocurrency, FinTech, InsurTech and regulation). Academic Press.

Date of project specification: 10.2.2022 ***Deadline for submission:*** 31.5.2022

Supervisor: Mgr. Jana Jašková, Ph.D.

doc. PhDr. Milena Krhutová, Ph.D.
Subject Council chairman

Abstract

Cryptocurrency has become a well-known phenomenon in the worlds of banking and electronic payments, but it is still a mystery to the general public, and not everything is explained so that anybody can trade with it. The focus of this thesis is on cryptocurrency. The study concentrates on the origins of cryptocurrencies, the principles on which their security works, why their transactions are untraceable, and how these transfers are carried out. Subsequently, the thesis deals with where the owner can store his cryptocurrencies, what types of wallets exist, what cryptocurrency mining deals with and what can be obtained through it. Individual cryptocurrencies are discussed in the second chapter of this thesis, including their history, and which wallets are appropriate for each coin. Furthermore, fiat currencies are discussed, including their history and the economic functions they perform. Lastly, these economic functions are applied to cryptocurrency. The purpose of this thesis is to gain a greater understanding of cryptocurrencies, including what they are, how they work, and how to deal with them as well as how they differ from fiat currency.

Keywords

Cryptocurrency, cryptography, blockchain, mining, Bitcoin, Ethereum, Dogecoin

Abstrakt

Kryptoměna se stala známým fenoménem ve světě bankovních a elektronických plateb, ale pro širokou veřejnost je stále záhadou, a ne vše je vysvětleno tak, aby s ní mohl kdokoliv obchodovat. Tato práce se zaměřuje na kryptoměny. Studie se zaměřuje na původ kryptoměn, principy, na kterých jejich zabezpečení funguje, proč jsou jejich transakce nevysledovatelné a jak jsou tyto převody prováděny. Následně se práce zabývá tím, kde může majitel uchovávat své kryptoměny, jaké typy peněženek existují, čím se těžba kryptoměn zabývá a co lze jejím prostřednictvím získat. Jednotlivé kryptoměny jsou diskutovány ke konci práce, včetně jejich historie a které peněženky jsou vhodné pro každou minci. Dále se tato práce věnuje fiat měnám, včetně jejich historie a ekonomických funkcí, které plní. Nakonec jsou tyto ekonomické funkce aplikovány na kryptoměny. Cílem této práce je získat větší přehled o kryptoměnách, včetně toho, co jsou zač, jak fungují a jak s nimi zacházet.

Klíčová slova

Kryptoměna, kryptografie, blokový řetězec, těžba, Bitcoin, Ethereum, Dogecoin

ROZŠÍŘENÝ ABSTRAKT

Kryptoměny mají významný dopad na globální ekonomiku, přesto se mnoho lidí s tímto konceptem neseznámilo a je pro ně velkou záhadou. Tato práce se zaměřuje na kryptoměny.

Historie bitcoinu je prvním tématem, kterému se věnuje první kapitola. Tato kapitola se zabývá původem bitcoinu, tím, kdo bitcoin založil, proč byla kryptoměna založena, a dramatem, které ji v průběhu historie provázelo.

V druhé části je rozebrán základní koncept bezpečnosti kryptoměn. Kryptografie je základem zabezpečení kryptoměn a skládá se ze dvou klíčů. Tyto klíče se nazývají veřejný a soukromý klíč. Tyto klíče jsou základními součástmi jakékoli formy kryptoměny. Fungují jako zámek a klíč. Sami o sobě jsou nepoužitelné, ale dohromady jsou kompletní.

První kapitola dále popisuje koncept Blockchainu. Tato část kapitoly zahrnuje vytvoření prvního Blockchainu a také široké pochopení toho, jak se bloky generují a co na nich může být uloženo.

Poslední část první kapitoly se zabývá těžbou, tím, co musí těžaři dělat, aby získali čerstvé mince, a konečně tím, kde a jak může člověk své mince schovat a uložit. Uložení kryptoměny je dále rozděleno do tří částí podle typu peněženky: softwarové peněženky, hardwarové peněženky, chladné peněženky a chladné úložiště.

Druhá kapitola se zaměřuje na tři různé kryptoměny. Jako první je zmíněn Bitcoin. Prvním tématem, kterému se tato podkapitola věnuje, je historie Bitcoinu a zajímavé události, k nimž došlo během jeho vzniku. Následně jsou vysvětleny čtyři samostatné peněženky, z nichž každá má vlastní soubor vlastností a kapacit pro zabezpečení měny dané osoby. Závěrečná část pojednává o použití Bitcoinu jako platební metody v reálném životě. Popisuje, jak se Bitcoin používá nelegálně i legálně.

Další probíranou kryptoměnou je Ethereum, po Bitcoinu druhá nejznámější kryptoměna. Tato podkapitola pojednává o koncepci, historii a vývoji Etherea. Dále je zde popsáno, které peněženky tuto minci podporují a jak ji lze využít v dnešním době.

Poslední probíranou kryptoměnou je Dogecoin. Tato kryptoměna není standardní mincí jako Bitcoin; jedná se spíše o altcoin, což je jakákoli mince odlišná od Bitcoinu, protože Bitcoin je původní kryptoměna. Tato podkapitola se zaměřuje na

zrození a následný vývoj Dogecoinu a také na významnou roli, kterou při jeho finančním růstu sehrál Elon Musk. Nakonec jsou zdůrazněny některé podporované peněženky a také uplatnění Dogecoinu v moderním životě.

Třetí kapitola se zaměřuje na fiat měnu, obecně známou jako reálné peníze, které jednotlivci využívají v každodenním životě. Tato kapitola začíná obecnou definicí fiat peněz a rozlišením mezi fiat a komoditními penězi.

Následující podkapitola se soustředí na historii fiat peněz, včetně toho, jaké byly první mince v Číně v 10. století, jak se tyto mince nakonec vyvinuly v papírové peníze a jak se v minulosti obchodovalo.

Nakonec jsou popsány tři hlavní ekonomické funkce, které fiat měna musí splnit, aby byla schopná úspěšně fungovat jako státní měna. První ekonomická funkce je známá jako prostředek směny. Tato část začíná definicí prostředku směny a popisem faktorů, které jej ovlivňují. Dále je charakterizován barterový systém, který byl v minulosti používán, a nakonec jsou popsány problémy, které se spojují s touto funkcí a fiat měnou.

Následující popsanou funkcí je zúčtovací jednotka. Tato podkapitola začíná základní definicí zúčtovací jednotky a následným popisem této funkce v reálných situacích. Pokračuje vysvětlením, proč fiat měny byli adoptovány jako zúčtovací jednotka a zakončuje popisem problémů, které přichází spolu s touto adaptací.

Poslední ekonomickou funkcí probíranou v této kapitole je uchovatel hodnoty. Tato podkapitola pojednává o tom, jak ekonomové definují uchovatele hodnoty, co je s touto funkcí spojeno a jaké vlastnosti musí měna splňovat, aby byla dobrým uchovatelem hodnoty. Nakonec tato podkapitola popisuje některé příklady toho, co je dobrým uchovatelem hodnoty, jako je na příklad zlato a jiné kovy.

Dříve zmíněné funkce jsou dále v závěrečné kapitole této bakalářské práce aplikovány na kryptoměny. U každé funkce je zkoumáno, zda jsou kryptoměna schopny vyhovět jejich požadavkům a pokud je splnit nedokáže, co se musí změnit, aby tuto funkci mohli vykonávat. Jelikož existují tisíce různých typů mincí, tato kapitola se u každé ekonomické funkce zaměřuje pouze na Bitcoin.

Bakalářská práce je zakončena závěrem, který shrnuje výsledky a myšlenky provedené během psaní práce. Hlavním cílem této práce je poskytnout čtenáři základní

informace týkající se toho, jak kryptoměny fungují, o čem pojednávají a jak se odlišují od běžných peněz.

Bibliographic citation

PETRENEC, Vojtěch. Kryptoměna – novodobý druh peněz [online]. Brno, 2022 [cit. 2022-05-31]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/142538. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav jazyků. Vedoucí práce Jana Jašková.

Author's Declaration

Author:	*Vojtěch Petrenec*
Author's ID:	*208998*
Paper type:	*Bachelor thesis*
Academic year:	*2021/22*
Topic:	*Cryptocurrency*

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

.

V Brně, 27 května, 2022 ----------

podpis autora

Acknowledgement

I would like to thank my supervisor, Mgr. Jana Jašková, Ph.D., for her invaluable pedagogical advice, support, and other valuable lessons I learned while writing this thesis.

Brno, May 27, 2022 ----------

Author’s signature

CONTENTS

INTRODUCTION

Money has always existed and will continue to exist in the future, and it is a force that drives the world whether a person likes it or not. What is fascinating is the evolution of money and how it has changed through time, despite the fact that its function has remained the same. If you asked ordinary people what kind of money they know, they would tell you anything from coins and printed money to zeroes on your debit card account, and the majority of these people have no economic education or are unconcerned about payment methods at all, but there is a small percentage who would tell you about cryptocurrency. The question is whether this small percentage understands what cryptocurrency is and how it works. The response is usually no; they may have heard of Bitcoin or cryptocurrencies, but only a small number of them understand what cryptocurrency stands for or how it is utilized and created.

Cryptocurrency is not something new it has been here for over 10 years, but nobody has been talking about it until millionaires started taking interest in it and the value of each cryptocurrency shifted and gained a significant value in the world of economics. In the past cryptocurrencies did not have that much of a meaning, some people might have had a certain amount, but they did not know what to do with it. Nowadays on the other hand people use it for all kinds of payments and since cryptocurrencies are untraceable not all the uses are for a good thing. It is important to study this subject and make it a common knowledge because it is going to enter our daily economy eventually and it needs to be better understood properly for people to use it freely without too many bad investments.

There are three primary chapters in this thesis. The first chapter begins with the historical events and setbacks that led to the development of cryptocurrencies as they are known today. It also discusses the most crucial technical components of cryptocurrencies. It will go over the security of cryptocurrencies, which is known as cryptography, as well as what Block-chain is and how a person may buy or mine cryptocurrency. This chapter will also discuss how cryptocurrencies are transferred, where they can be stored, and what kinds of wallets could be used to keep them.

The second chapter focuses on particular cryptocurrencies such as Bitcoin, Ethereum, and Dogecoin. It will discuss how they contributed to the rise in the world of

the cryptoverse, what difficulties they had to overcome to achieve the price and the name they now carry, and which wallet is preferable for each cryptocurrency.

The third chapter focuses on fiat currency, sometimes known as "real money" and used by individuals on a daily basis. It starts with a general explanation of fiat money, then goes on to explain the difference between fiat and commodity money, and finally goes over the history of fiat money. Furthermore, three economic functions are described at the end of the chapter.

The final chapter's major aim is to determine whether cryptocurrencies may be utilised in the same way that fiat money can. To accomplish this, the three previously mentioned economic functions were applied to cryptocurrencies.

1. CRYPTOCURRENCY

The phrase cryptocurrency has become widely utilized in financial circles, new company concepts, and news headlines in recent years. Since it is untraceable and virtually hard to counterfeit or double-spend, it is frequently associated with criminal activity on the so-called "dark web." The phrase crypto, the idea what it is, and its goods are now entering public knowledge, thanks to the soaring value of currencies like Bitcoin. (Furneaux, 2018, p. 3) This chapter looks at the idea, its technology, history, and applications of cryptocurrencies.

1.1 History of cryptocurrency

David Chaum, a talented cryptographer, was the catalyst for the whole event. He was a United States citizen who was born in Los Angeles, California, in 1955 to a rich Jewish family. He was a talented mathematician who insisted on having his way all the time. He journeyed around the world when he was in his thirties, arriving in Amsterdam at the end of his journey. He became a member of a CWI (College of Western Idaho) department team of cryptographers. There, he collaborated on electronic payment systems with a few other researchers. Rijkswaterstaat (Dutch Department of Public Works) became interested in the early 1990s when they were considering implementing automatic toll-collection roads. David and his classmates seized the opportunity and accepted the work, which they completed in less than a week. They formed DigiCash in 1990 as a result of their collaboration. (How DigiCash Blew Everything, 1999)

While pursuing other projects in 1993 he invented digital payment system Ecash. This system was first ever technically perfect product which made it possible to pay over the Internet safely and anonymously. Ecash users would obtain their electronic money by downloading it from their bank. It would then be saved on their computer by a software until they were ready to utilize it. Those dollars were, in fact, a string of numbers.

According to Gerstein (2021) the strings were then mixed by adding a random number to them. The digital coins were sent to the bank afterwards, which blindly signed them while also deducting one real dollar from the user's account for each signed coin. When a customer placed an online order, the vendor just had to check with the

bank to ensure that the coins were signed by a bank and had never been used before. Because of this manoeuvre, neither the seller nor the bank knew who bought what, resulting in anonymity and no evidence of a person's payment. DigiCash went bankrupt in 1998, but at that time, Deutsche Bank and an American financial institution called Mark Twain Bank had acquired about 5,000 users. Bill Gates, Visa, and investment firms were also rumoured to be interested, but nothing came of it. In many aspects, DigiCash and its Ecash payment system are forerunners to Bitcoin.

In 2009, a year after the global economic crisis that affected everyone, the first cryptocurrency, bitcoin, was developed. The founder, nicknamed Satoshi Nakamoto, is still unknown, and he is doing an excellent job of concealing his identity. Several people have been suggested as Satoshi Nakamoto, but none has been proven to be Satoshi Nakamoto beyond a reasonable doubt, hence Satoshi's identity has remained a mystery despite several attempts to track him down. (Baldridge, 2021)

The philosophy behind bitcoin might be the most significant component of it. Satoshi noticed certain significant faults in existing payment methods and, rather than developing an entirely new payment method that would radically disrupt the way people pay for things, he attempted to correct them. The fact that the development occurred shortly after the global financial crisis was no coincidence. After the crisis, every financial system was on the verge of collapsing, and many banks began to engage in quantitative easing. That is when a central bank buys a specific amount of government bonds or other financial assets to infuse money into the economy and boost economic activity. Interest rates were slashed to near zero thanks to quantitative easing in order to avert the Great Depression of the 1930s.

According to Prypto (2016, p. 7) after seeing what central banks had done, Satoshi decided it was time for a new monetary system, one that was so distinct from existing infrastructure that it might even be labelled as disruptive. Despite the fact that it is uncertain if bitcoin was ever meant to totally replace financial infrastructure, several institutions are investigating the technology that underpins Bitcoin because they see its potential and want to utilize it for their own purposes. Finally, bitcoin is more than simply a new payment mechanism; it also has a guiding ideology: it is about utilizing the underlying technology to its utmost potential and assisting one another. Decentralization is one of the major concepts underpinning Bitcoin, which implies that

everyone participates in the bitcoin ecosystem and contributes in their own unique way, rather than relying on the government or banks. Bitcoin belongs to everyone, and this system is known as peer-to-peer.

1.2 Cryptography

Every cryptocurrency must go through several safety elements in order to be untraceable and secure. The sender must first encrypt the message, which makes the content unreadable to third parties, and then the receiver must decrypt the message, making it readable once more. Cryptography is used to enable these security characteristics. Both cryptography and cryptocurrency have the term "crypto" in their names, as their names imply. This phrase means "secret" in Greek, and that is precisely what cryptography is about: exchanging safe, encrypted communications or data between two or more people. The finest part is that in order for a transaction to be secure, the one making the transaction does not need to know anything about the person receiving it. In the middle of the transaction, there is no need for bank information, credit card numbers, or any other third party. This function is important not just when dealing with cryptocurrency, but also when sending an e-mail, searching for something on Google, or if your computer has a problem. A transmission between a network and its linked computers is constantly encrypted and decrypted by the computer. (What is cryptography?)

1.2.1 Public-private key encryption

To better comprehend cryptography and why it is so vital, one must first comprehend what a public and private key is, as well as how encryption works. Public and private keys are essential components of any cryptocurrency, regardless of the kind. They let users to transmit and receive cryptocurrencies without the need for a third party to verify the transaction. A person may transmit his Bitcoin to anybody, anywhere, at any time with these keys. These two keys serve as a lock and a key; alone, they are worthless, but together, they open a door to your transaction. On the one hand, the public key may be shared with everyone to receive transactions, while the private key must be kept private. If a person’s private keys are stolen, anybody with access to them will be able to access any cryptocurrency linked to those keys. (Cryptopedia Staff, 2021)

As it is mentioned in last paragraph the public key can be distributed to anyone and anyone can use it for encryption. It can be looked at as business address on the web, anybody can search it up and share it widely. You can neither decipher nor infer the original content of the data from the ciphertext, nor can you use the same key to unlock it once the data has been encrypted using a public key. Complex asymmetric encryption methods are used to produce your public key. There are many distinct sorts of algorithms in these approaches, and each type decides how long the public key will be. The key size ranges from 128 bits to 4096 bits in general. (Mehta, 2020)

Mehta(2020) claims that each public key has a private key that corresponds to it. This key is capable of decrypting ciphered data (i.e., encrypted data). Each pair of public and private keys is distinct. It is important to keep the private key secret and stored somewhere safely. The best approach to keep data safe is to keep it on an approved device or a server that is not accessible to the public. Even though the key is private, the person who has it must keep it secure and know where it is at all times. If this individual loses this key, he will have a lot of work ahead of him since he will need to re-issue his certificate. Because a private key is produced with high entropy (randomness), guessing it from its associated public key is extremely difficult, which means that even the most powerful computer would take thousands of years to interpret this private key using brute force. That being stated, only an approved device that contains the private key should be able to decode this data.

1.3 Blockchain

A blockchain can be thought of as a ledger with records of transactions or contracts that are shared across many nodes on a network, so it is more of a database than software (Investigating Cryptocurrencies, p.39). According to Conway (2021) it keeps encrypted data in electronic form in a digital format. Blockchain plays an important role in cryptocurrencies, because it keeps a secure and decentralized record of transactions. The blockchain's uniqueness is that it ensures the loyalty and security of a data record while also generating trust without the requirement for a trusted third party. The way it is being structured is the key difference between a normal database and a blockchain. The blockchain collects data into what is known as "blocks," which might contain different types of information, but most common is ledger of transactions. A

block can be thought of as a box packed with information, with a specific amount of storage space, and once that capacity is filled, a new box is required for storage, and collectively these boxes form a chain, which is why it is called blockchain. When implemented in a decentralized manner, this data structure creates an irreversible chronology of data. When a block is completed, it is imprinted in stone and becomes a part of this chronology. When a block is added to the chain, it is assigned a precise timestamp. When a block is filled with data, it is effectively locked and nothing may be altered, deleted, or destroyed. The transaction method is simple: a new transaction is created, which is then communicated to a global network of peer-to-peer computers. This network then employs public-private key encryption to solve equations in order to certify the transaction's legitimacy. After confirming that the transaction is valid, the data is grouped into blocks. These blocks then chain together to build a blockchain with a long history of all permanent transactions. The transaction is then finished.

Conway (2021) also mentions that if a person imagines a corporation that uses a server database and has a storage facility with thousands of computers with customer account information safely stored on these machines under one roof. The firm is in charge of everything, but there is one shortcoming that blockchain does not have. If the power would go out, the internet would be down, or, in the worst-case scenario, if the entire warehouse burned down, everything would be lost. In either situation, the data has been lost or distorted. As previously stated, blockchain enables data held in databases to be shared across network nodes of peer-to-peer computers located in diverse locations. Thanks to this the database is more redundant and it also ensures the accuracy of the data contained there. Also, if someone tries to update a record in one instance of the database, it will have no effect on the other nodes, which will remain unchanged. This would then result in a process known as cross-reference between each node, resulting in the tempered node being pinpointed with inaccurate information. It is safe to say that no node can change the information it holds as a result of this process.

1.4 Mining and Miners

The cause for the surge in demand for graphics processing units (GPU) in recent years has been cryptocurrency mining. The mining gold rush was short-lived since mining cryptocurrencies such as Bitcoin became more difficult. However, the demand

for GPUs remains high, which suggests that cryptocurrency mining may still be worthwhile. The majority of people consider crypto mining to be nothing more than a method of manufacturing new currency. Crypto mining, on the other hand, entails validating bitcoin transactions and adding them to a distributed ledger on a blockchain network. Most crucially, crypto mining prevents digital currency from being spent twice on a decentralized network. The mining process is critical for validating transactions since distributed ledgers lack a central authority. Miners are thus motivated to safeguard the network by taking part in the transaction validation process, which enhances their chances of winning newly generated coins. Miners must deploy devices that solve complicated mathematical equations in the form of cryptographic hashes in order to be rewarded with new coins.

A proof-of-work (PoW) consensus system has been implemented to ensure that only certified miners can mine and validate transactions. PoW also protects the network against outside threats. Cryptocurrency mining necessitates the use of computers with specialized software designed to solve complex cryptographic equations. Cryptocurrencies like Bitcoin may be mined with a simple CPU chip on a home computer in the early days of the technology. Mining cryptocurrency today necessitates the use of a specialized GPU or an application-specific integrated circuit. Most governments and authorities have to implement legislation governing crypto mining, therefore the legality of crypto mining in most nations is still up in the air.

The Financial Crimes Enforcement Network classifies miners as money transmitters. Cryptocurrency miners may be subject to the same laws as money transmitters, requiring them to follow the same rules as financial institutions. Crypto mining is considered as a business in Israel and is subject to corporate income tax, although regulatory uncertainty continues in India and elsewhere. Only a few countries prohibit crypto mining, with the exception of jurisdictions that have officially prohibited cryptocurrency-related activities. (*What Is Crypto Mining?*)

1.5 Storage

If a person has a cryptocurrency, such as Bitcoin, the first thing that comes to mind is that he needs to put it somewhere. Most individuals believe that he or she can use a secure digital wallet to receive and send cryptocurrency, but they are mistaken.

According to Furneax (2018, p. 95) a digital wallet does not really contain bitcoin or any other cryptocurrency, and because it does not, it cannot transfer or receive it. What a digital wallet does is keep a list of private and public keys that it can resolve. The wallet simply creates a balance from the transactions it can control by either observing a local copy of the blockchain or interacting with a copy belonging to another full-node user. There are various sorts of cryptocurrency wallets, ranging from software wallets to hardware wallets to a piece of paper. Even if a person writes his private key on a piece of paper, it is still officially referred to be a wallet.

1.5.1 Software Wallets

Furneax (2018, p. 97) also claims that software wallets are divided into three categories. Full Node Wallet is the first. This wallet has downloaded the whole blockchain, which means transactions are processed and confirmed locally before being sent to peers. The Thin Node Wallet falls into the second category, with its client connecting to another full node for transaction processing. An Online Wallet is the third and final category. The wallet, as the name implies, is only available on an online wallet site. The important distinction here is that the transaction data is not often linked to a local client. There are several software wallets choices, the most popular are for instance: Bitcoin Core, Electrum, Bitcoin Knots, Bither and many others. They all have different traits and powers; therefore they must be carefully picked. Many of these wallets rely on operating system security, which means that if a person knows the system password or can image the halted device, he may easily access the wallet and its contents.

1.5.2 Hardware Wallets

On the other hand, hardware wallets are as the name suggest wallets that store a private key and things like account balance on physical devices. These types of wallets are generally exceedingly secure. If stolen, unlocking them almost always requires owner's assistance. In the event that a person loses PIN or misplaces the device, each of these wallets has a recovery feature. These are some excellent examples of hardware wallets, but as with software wallets, each has its own set of advantages and disadvantages to consider: KeepKey, Ledger Nano X, Trezor Model T. (Furneaux, 2018, p. 97)

1.5.3 Cold wallets and Cold storage

Furneax (2018, p. 98) points out that a wallet has nothing to do with the storage of actual coins, but rather with the backup of a person's private keys in some sort of ledger. This means that if a person wants to store a private key without purchasing a wallet, they can simply write it on a piece of paper and hide it in a safe place. A private key on a piece of paper is a good example of cold storage. Cold storage is any type of storage, not just a piece of paper, that keeps a person's private keys offline, which means they don't need to be connected to the internet to keep a person's coins safe. A USB key, a piece of paper, or a hardware wallet can all be used for cold storage. Even if the cold wallets are offline, they can still accept coins from senders because they only receive an address stored on the blockchain rather than a currency. Even while this wallet can receive coins and so grow in wealth, it cannot send funds out until it is plugged into or imported into a wallet that can.

2. INDIVIDUAL CRYPTOCURRENCIES

This part of the thesis focuses on individual cryptocurrencies. It will mention their beginning and development, where they can be stored and the utilization in today's market. The first cryptocurrency that will be described is Bitcoin.

2.1 Bitcoin

According to Ashford and Curry (2021) Bitcoin is not only the first cryptocurrency, but also the most famous of the more than 5,000 cryptocurrencies now in use. Bitcoin is decentralised digital money that can be bought, sold, and exchanged without the use of an intermediary such as a bank. Each Bitcoin transaction is recorded in a public ledger that is accessible to all, making it impossible to reverse and forge the transactions. Bitcoins are not covered by the government, or any other emission organisation and their value is only guaranteed by the evidence that is part of the system.

2.1.1 History of Bitcoin

Satoshi Nakamoto first introduced Bitcoin in 2008, when he published the White paper "Bitcoin: A Peer-to-Peer Electronic Cash System," which explains how the Bitcoin blockchain network works. Satoshi Nakamoto, whose true identity is still unknown, mined the first block of the Bitcoin network four months later, effectively launching the blockchain technology. The Genesis Block is the first block to be mined. The first ever purchase was made by Laszlo Hanyecz, who bought two pizzas for 10,000 BTC. This day is commemorated as the Bitcoin Pizza Day. Following the emergence of Bitcoin as the world's first cryptocurrency, there was a need to find a solution to the transaction in order for a cryptocurrency market to emerge. A website called bitcoinmarket.com, which is now defunct, made the first cryptocurrency trade-off in March 2010. Mt. Gox, the first bitcoin exchange company, was founded the same year. Between 2011 and 2013, Bitcoin was able to equalise with the US Dollar in February. Several competing cryptocurrencies have debuted that year. (A brief history of bitcoin & cryptocurrency, 2019)

With the following growth of Bitcoin value, the first hacks emerged. In June 2011, Mt. Gox had been hacked for the first time with the valued loss of 2,000 BTC

which had value around $30,000 at the time. Mt.Gox was the first major cryptocurrency exchange to be hacked in 2014, with 850,000 BTC stolen. This is the greatest Bitcoin theft in history, with a total value of $460 million at the time. Following this, the price of Bitcoin dropped by 50% and would not recover until late 2016. Despite other annoyances like as different hacker assaults, Bitcoin theft, and the prohibition of Bitcoins in China, the price of Bitcoin fluctuates but continues to rise. (A brief history of bitcoin & cryptocurrency, 2019)

2.1.2 Wallets

According to Conway (2021) a good place to start with bitcoin wallets for an inexperienced would-be Exodus. This wallet is mobile and desktop compatible, and the user interface is straightforward and easy to use thanks to the built-in exchange system, which allows you to choose from 150 different cryptocurrencies.

Electrum is the ideal desktop wallet for advanced bitcoin traders since it is free, has configurable transaction fees, and has superior security than other cloud wallets. This wallet, on the other hand, only supports software wallets, the user interface is more focused on the work at hand, and as a result of its numerous possibilities, it is also more suitable for experienced users.

Mycelium is the finest Bitcoin wallet for mobile users since it includes configurable transaction fees like Electrum but also supports the use of hardware wallets and is more user pleasant.

The leading paid hardware option on the market right now is the Ledger Nano X, which can be connected via USB drive or Bluetooth connecter. Although the Bluetooth option has been hacked in the past, it allows users to connect to their Ledger without the use of a computer. Trezor Model T is a more secure solution, however it has less user-friendly controls and costs more.

2.1.3 Usage of Bitcoin

Chapman (2018) claims that Bitcoin has a terrible reputation for being used by terrorists or criminals with malevolent motives who buy or trade illicit guns or drugs. For marketplaces like Silk Road, which is now defunct, and its more current clones, the sole choice is to transmit and receive bitcoin for the same reason: cryptocurrencies like

Bitcoin are untraceable. Normal transactions involving a bank account or printed money are no longer worthwhile to them because they may now be traceable.

It is becoming increasingly easier for people with no malicious intentions to spend as much money as they want online. Several online merchants, including Microsoft/Xbox, Namecheap, Newegg, Overstock, and Shopify, now allow consumers to fund their accounts with Bitcoin or other cryptocurrencies. AT&T, Dish Network, Namecheap, ProtonMail, Twitch, and even Wikipedia all accepted Bitcoin payments, either directly or through third-party service providers. Today, Bitcoin can even be used to even pay for education. For its online executive education program, the University of Pennsylvania's Wharton School has recently begun taking cryptocurrency. (Spilka, 2018)

2.2 Ethereum

Marr (2018) defines Ethereum as an open-source public service that makes use of blockchain technology to enable smart contracts and cryptocurrency trading without the need for a middleman. The two types of accounts available on Ethereum are externally owned accounts (controlled by private keys affected by human users) and contract accounts. Ethereum gives programmers the ability to design a wide range of decentralised apps. Despite the fact that Bitcoin is still the most favourable and has the highest price, Ethereum is rapidly rising and may soon replace Bitcoin in terms of usage.

2.2.1 History of Ethereum

According to Marr (2018), Ethereum was initially described by Vitalik Buterin in late 2013 as a result of his research and work in the Bitcoin community. He had different vision from Bitcoin community and decided they weren’t approaching the problem in the right way. He started to imagine a platform that went beyond the financial use cases allowed by Bitcoin and released a white paper in 2013 describing what would ultimately become Ethereum using a general scripting language. The key differentiator from Bitcoin was the platform’s ability to trade more than just cryptocurrency.

Marr (2018) claims that Buterin and his co-founders launched a crowdsourcing effort in 2014. This campaign sold Ether, an Ethereum currency, to participants in order

to accelerate their concept. The total amount raised was more than eighteen million US dollars. The first live version of Ethereum was nicknamed Frontier, and it was released in 2015. From there, the platform grew swiftly, and hundreds of developers are now involved in the process. Similarly, to how hackers first arrived when Bitcoin was in its early stages, when Ethereum was blooming, the first hackers appeared. An unknown group of hackers stole fifty million dollars in June 2016, raising security worries. This provoked a hard fork, which resulted in a split in the Ethereum community and the formation of two different blockchains: Ethereum (ETH) and Ethereum Classic (ETC).

Wu (2021) claims that from 2017 to the present, Ethereum has been overcoming difficulties in terms of security, privacy, scalability, and sustainability. The most recent versions are aimed at a broader audience without encountering security problems or high-level difficulties. The Ethereum community is forward-thinking, having adopted multiple substantial modifications over time. It overcame numerous hurdles during its scaling process and is looking optimistically about their future.

2.2.2 Wallets

Many wallets that are usable by Bitcoin can also be used to store other cryptocurrencies. As previously stated, the Exodus option is a fantastic place to start for newcomers. Exodus may be downloaded on both mobile and desktop devices, and it supports 150 different cryptocurrencies.

Mist, an official Ethereum wallet, is a popular choice in software desktop wallets. On the one side, this wallet was created by its authors, which implies it is officially endorsed and supported; on the other hand, it is less user friendly than other wallets.

Mycelium, which has previously been mentioned as a mobile wallet option, is available, but if you want to work with ETC, it is not supported. To exchange, buy, or sell ETC, the best wallet to use is Coinomi, which also prioritises privacy.

The Ledger NanoX, as previously stated, is the industry leader in hardware wallets, but the KeepKey, which has comparable capabilities but a slightly larger screen, is an excellent option. As indicated earlier, a hardware wallet like Trezor, which has a solid reputation and supports nearly 700 different coins and tokens, is a much safer option. (Solomon 2019)

2.2.3 Usage of Ethereum

Unlike Bitcoin, Ethereum is more than just a digital asset. Ethereum is a platform on which a variety of Blockchain-related applications can be created, allowing for a wide range of Ethereum spending options. ETH can be exchanged for Bitcoin or any other cryptocurrency. Purchasing or selling these coins in the expectation of reaping a large profit has become commonplace. Another option is to take part in an initial coin offering (ICO). An ICO, is a method by which a new enterprise sells its newly created crypto tokens, usually in exchange for Bitcoin or Ethereum IPOs are intended to provide start-ups with the necessary venture money to bring their ideas to life. Another option for spending Ethereum is to trade it for any service or item, as it may be traded with anyone who has a linked wallet address. The final option is to swap ETH for actual money, but he or she should be aware that in most countries, any exchange of ETH for real money will be considered a taxable event. (*What Can I Buy with Ethereum?*)

2.3 Dogecoin

Frankenfield (2021) claims that DOGE is a cryptocurrency that is peer-to-peer and has open-source code. It's an altcoin that's more of a sarcastic meme coin. The term "altcoins" refers to all cryptocurrencies other than Bitcoin. Its emblem is a Shiba Inu, a popular meme dog. Dogecoins blockchain has justification, despite the fact that it was designed more as a joke. His primary technology is based on Litecoin. Dogecoin, which employs an algorithm script, is notable for its low prices and limitless supply. It is an "inflationary coin," while cryptocurrencies like Bitcoin are deflationary because there is a ceiling on the number of coins that will be created. Every four years, the amount of Bitcoin released into circulation via mining rewards is halved, and its inflation rate is halved along with it until all coins are released.

2.3.1 History of Dogecoin¨

Dogecoin was invented in 2013 by Jackson Palmer, a product manager at Adobe Inc.'s Australian branch, as a satire of the cryptocurrency mania. Meanwhile, in Portland, Billy Markus, an IBM software developer who wanted to start his own cryptocurrency but was having trouble with promotion, noticed the Dogecoin frenzy. Markus has contacted Palmer to request permission to develop software that will be

used to back up a real Dogecoin. On December 6th, 2013, Palmer and Markus released the coin to the public. Dogecoin's value soared by 300 percent in under two weeks, starting December 19th. China's banks were restricted from investing in cryptocurrencies, which could be the reason for this growth. (Frankenfield, 2021)

According to Frankenfield (2021) in 2015, the Dogecoin community's former spirit of humor began to dissolve as the overall crypto community became more serious. The first indicator that the Dogecoin community was in trouble was the resignation of its founder, Jackson Palmer, who claimed that a poisonous community had sprung up around the coin and money it generated. Alex Green, alias Ryan Kennedy, a British man who founded the Dogecoin exchange Moolah, was one of the toxic members of the community. Green was able to persuade other members of the community to donate huge quantities of money to help fund the development of his exchange. These donations were eventually proven to have been used to purchase more than 1.5 million dollars in Bitcoins for his own gain and use, rather than for the creation of his exchange.

Frankenfield (2021) says that during the cryptocurrency boom, Dogecoin's value rose along with other cryptocurrencies, peaked at the end of 2017, and has since been decreasing along with other cryptocurrencies in 2018. In the summer of 2019, Dogecoin, like other coins, saw a rise in value. Dogecoin supporters were overjoyed when the crypto market Binance listed the coin, and many assumed that Tesla CEO Elon Musk had backed the coin in his mysterious tweet, causing the coin's value to skyrocket.

Musk continued to back Dogecoin in 2021, tweeting in May that he was collaborating with the coin's developers on improving transaction efficiency. With a market capitalization of $31.9 billion, Dogecoin was ranked 10th in the market cap rankings, up from 48th and $339 million the previous year. (Frankenfield, 2021)

2.3.2 Wallets

Because Dogecoin is an altcoin, most wallets designed for Bitcoin and Ethereum will not work with it, with the exception of Ledger NanoX and Trezor, which are still the best hardware wallets available.

According to Thompson (2021), there are various software wallet options, one of which is Binance, one of the top Dogecoin wallets that allows you to create a digital wallet and trade over 150 cryptocurrencies on a single platform. It also comes with an

API that you can use to integrate it with your current trading platform. CoinBase is another option, which is more beginner-friendly but not available everywhere.

2.3.3 Usage of Dogecoin

Gupta (2021) points out that, Dogecoin can be spent in a variety of ways, just like Ethereum and Bitcoin. The first option is to spend it in online stores that accept this kind of payment, as well as in restaurants, travel agencies, and videogame stores. On Twitter or Reddit, a person can show their support for their favourite content creator. Dogecoin is now accepted as payment by dozens of businesses, including Kronos Advanced Technologies, Iron Rail Diner, AllGamer.net, Travala.com, and NinjaGameKeys. Although crypto exchanges such as bitcoin and ether do not now allow dogecoin, a growing number of prominent platforms are beginning to do so.

3. FIAT CURRENCY

To completely comprehend the similarities and differences between paper money and cryptocurrencies, it is necessary to fully understand what the concept "fiat currency" implies, what its attributes are, and how they function. This chapter of the thesis will explain fiat currencies, as well as what functions fiat currencies must fulfil in order to function correctly as money in the economy.

3.1 Understanding fiat currency

Fiat money, according to Chen (2022), is a government-created currency that is not protected by a physical commodity like gold or silver, but rather by the government that issued it. Fiat currency's value is determined by the connection between supply and demand as well as the stability of the government that issues it, not by the value of the commodity that backs it. The majority of current paper currencies, including the US dollar, the euro, and many other major currencies, are fiat currencies.

The term "fiat" originates in Latin and is commonly interpreted as "it shall be" or "let it be done." This is a close translation to what actually occurs. The only reason fiat currencies have value is because the government chooses what that value is and then does everything possible to maintain that value, implying that fiat money has no benefit in and of itself. (Chen, 2022)

Chen (2022) further points out that most currencies in the past were representational currencies, meaning they were backed by gold or silver. This meant that each piece of paper money was worth a specific amount of gold or silver. This also implies that the government should only be authorized to print a set amount of paper money based on the amount of gold or silver within their vaults. This would enable a person to go to a bank and exchange paper cash, such as a dollar, for dollars' worth of gold. Convertibility is the term for this ability. Fiat, on the other hand, is inconvertible and cannot be redeemed because it is backed by no underlying commodity.

In order to better understand what fiat currencies are, it is important to comprehend what is the difference between fiat money and commodity money

3.1.1 Difference between fiat money and commodity money

According to Charm (2016), a legal claim is fiat money since it gets all of its attributes from the law. It works similarly to a purchase voucher in a way that it may be traded for goods and services and has varying purchasing power. The settlement of debts is the sole fixed privilege linked with fiat money. It was first developed as a convenient form of currency that allowed people to carry paper which was supported by government instead of having gold or silver in their pockets. As time passed, governments stopped backing up their fiat money with gold or other forms of commodities, and it lost its initial value. Because fiat currency is essentially worthless, it cannot be exchanged for anything other than other fiat currency.

Commodity money, to the contrary, is money that receives its value from the goods from which it is made. It is possible to request that commodity money be exchanged for specific goods. Commodities used as a medium of exchange include gold, silver, copper, valuable stones, and even alcohol and tobacco. The gold standard is an excellent example of a commodity currency. It is a monetary system in which a country's currency or paper money has a direct link to gold. The goal of commodity money was to make it easier to trade rather than to employ the barter trade system, which is based on simple exchange without the use of any form of money (Charm, 2016).

Charm (2016) also claims that commodity currency is money that is considered to be a contemporary goods. Fiat money, on the other hand, is a future liability because it only promises to pay in the future. When it comes to fiat money, payment is never made; rather, it is discharged. Commodity money, on the other hand, completes the transaction. The final payment in the commodity money system is always made in the form of a commodity that is used as money in the transaction. Fiat money is paper money that represents only a promise or a liability. Under the fiat money system, there will never be a final payment because the transaction is made with the promise, representation, or commitment that something else must be paid.

3.1.2 History and development

"Fiat Money: What is Fiat Money?" (n.d.) states that the creation of fiat currency began in China in the 10th century, mostly during the dynasties of Jüan, Tchang, Sung, and Ming. It all started during the Tchang Dynasty (618–907), when the demand for

metallic currency outstripped the availability of precious metals. People became accustomed to using credit notes throughout this time period and were willing to accept scraps of paper or paper drafts. There were no coins, because precious metals were in short supply, forcing people to switch from coins to banknotes. During the Song Dynasty (960–1276), the Sichuan region experienced a tremendous increase in business, resulting in a scarcity of copper coins. As a result, merchants began to issue private notes backed by monetary reserve, which were regarded as the first legal tender. Later, during the Yuan Dynasty (1276–1367), paper money was the only legal tender available for use, and during the Ming Dynasty (1368–1644), the Ministry of Finance was given the authority to issue banknotes.

"Fiat Money: What is Fiat Money?" (n.d.) suggests that in the 18th century, the western part of the world began to use paper money. The Continental Congress, the American colonies and France began issuing bills that were used for payments. The provincial governments produced notes to be used to pay taxes to the authorities. Because of the risks of inflation, issuing too many bills of credit sparked some debate. The bills decreased in value dramatically in some locations, such as New England and the Carolinas, which resulted in a rise in commodities prices as the price of bills declined. Countries use fiat currencies to protect the merits of precious metals like gold and silver during wartime. For instance, during the American Civil War, the Federal Government of the United States utilized a sort of fiat currency known as "Greenbacks." During the war, the government stopped issuing paper money that could be exchanged for gold or silver.

At the beginning of the 20th century, the government and banks had pledged that banknotes and coins will be available on demand to exchange for their nominal commodity. The government was compelled to cancel the redemption due to the tremendous cost of the American Civil War and the necessity to reconstruct the economy. In 1944 The Bretton Woods Agreement was settled. The main purpose of this agreement was to find a solution for the prevailing issues that plagued currency exchange. This agreement set the price of a troy ounce of gold at $35 US dollars. The failure of this agreement began when, US President Richard Nixon presented a series of economic actions in 1971 due to falling gold reserves. The main action involved the cancellation of direct convertibility of dollars into gold. Afterwards, the vast majority of

countries have adopted fiat currencies that can be exchanged for major currencies ("Fiat Money: What is Fiat Money?" n.d.).

3.2 Functions

Nasrudin (2022) claims that for a fiat currency to function properly as money in an economy, it must first be able to perform three functions. These are the functions of a medium of exchange, a unit of account, and a store of value.

3.2.1 Medium of exchange

According to Chen (2020), a medium of exchange is a tool or system that acts as a middleman between parties to facilitate the sale, purchase, or exchange of products. To function as a medium of trade, this system must represent a standard of value, and this standard must be accepted by all parties. The economy will be more efficient as a result of adopting the medium of exchange, and it will also drive an increase in general trading activity. Trade was only possible in the old barter system if one of the parties had what the other desired, and vice versa. This is where gold comes into play because the chances of this happening are rather slim. The problem with the barter system would be overcome if gold was utilized as a medium of exchange. For example, if a farmer has a cow and decides he no longer wants it but needs a lawnmower, he could try to trade his cow for a lawnmower but finding someone willing to do so is unlikely. Instead of trying to locate someone who would accept this bargain, he could sell his cow for gold and then buy his lawnmower, making gold the medium of exchange in this transaction.

Anyone who is in possession of money has the ability to participate in the market on an equal footing. When people use money to buy something or get a service, they are effectively making a bid in response to a price that has been set. In the marketplace, this interplay provides order and predictability. Consumers can organize their budgets around predictable and stable pricing models, while producers know what to produce and how much to charge. Consumers lose their ability to arrange budgets when money, as represented by a currency, is no longer viable as a means of exchange or when its monetary units can no longer be accurately valued. Furthermore, precise supply and demand estimation is no longer possible. In a sense, market volatility will wreak havoc on the markets (Chen, 2020).

3.2.2 Unit of account

Mesk (n.d.) claims that this function could be simply referred to as a measurement of value. It is essentially a way to measure the value of anything. It could be associated with cryptocurrencies, fiat currencies, or any other tool that allows a person to contrast the worth of other items. The phrase is used in economics to express one of money's most important functions, which is to assess the worth of a certain property, good, or service. This property enables people to compare the monetary values of a variety of products using a specific currency, such as the US Dollar, the British Pound, or the Euro.

As it was mentioned at the beginning of previous paragraph, this function can be referred to as a type of measurement of a certain value, so for instance, the same way people use centimeters to measure distance and length, a unit of account is used to determine the monetary value of almost anything. A money property like this allows us to compare the worth of a car to the value of a house, for example. Another example would be comparing oranges with apples, even though they are very distinct. Money is utilized as a unit of account since it is employed to measure practically everything people produce and consume. Mesk (n. d.) also mentions that unit of account is what enables money to be lent and borrowed, as well as granting the ability to undertake mathematical operations, such as calculating gains, losses, and income. To put it another way, this property of money is what provides the numerical value and meaning behind products and services which people create, exchange, and consume.

However, due to inflation, deflation, and other economic factors, the value of money in real life is highly volatile. As a result, money is not always seen as a suitable unit of account because its ability to assess the value of things varies. A good example for better understanding is if the unit of a centimeter could not hold constant across time, the centimeter would thereafter become less and less valuable as a unit for measuring distance or length. (Mesk, n.d.)

3.2.3 Store of value

Downey (2021) defines a store of value as a term that refers to the ability of an item, commodity, or currency to be kept, retrieved, and exchanged in the future without losing value. A good store of value, according to "Store of Value" (n.d.), is one that allows its owner to sell or trade it at a later point for a similar or better value than when

it was first purchased. This worth is usually determined by the asset's market price or purchasing power (monetary value). However, it could also be tied to the asset's liquidity in specific situations. The term "liquidity" is defined by "Liquidity" (n.d.) as the ability to sell or buy an asset without having a significant impact on the market price. It also has to do with the ease with which an asset can be converted into fiat currency. Property or assets that are difficult to convert to cash are not considered liquid, but those that may be traded immediately are.

A moderately stable currency, according to Downey (2021), is necessary for a functioning economy. In order for residents to engage in work and commerce, save money, and spend it, a country's currency must be a legitimate store of value. A monetary unit that fails to act as a store of value eliminates the incentive to save or even earn money, as well as reducing the ability to trade.

Anonymous (n.d.) states that inflation has eroded the purchase power of most fiat currencies for a long time (mostly due to a rapid increase in the circulating supply of that currency). Despite the impacts of inflation, many economists regard money as the most basic example of a store of value. It's possible that this is linked to its purchasing power, which fluctuates relatively slowly. Money is perhaps the most liquid financial instrument we have right now. Even so, claiming that money is a good store of value is debatable. Mostly because depreciation is constantly caused by inflation and hyperinflation

Gold and other metals, according to Downey (2021), are great stores of value since their life span are basically infinite. Interest-bearing assets, such as US Treasury bonds (T-bonds), can qualify for shareholders and investors because they maintain their value while producing income. Milk, on the other hand, is a poor store of value since it spoils and loses its value over time.

Some people regard Bitcoin as an excellent store of value, and it is frequently referred to as "digital gold." Bitcoin is rare and unbreakable. As it is mentioned before in this thesis, it is a type of digital money that can't be duplicated or spent twice. These are some of the primary reasons why Bitcoin's value rises over time. However, some contend that Bitcoin is not a store of value by the definition due to its high volatility and volatile market price (Anonymous, n.d.).

4. FUNCTIONS OF FIAT CURRENCIES APPLIED TO CRYPTOCURRENCY

Considering fiat currencies differ from cryptocurrencies in many ways, it is vital to assess whether cryptocurrencies can adequately perform economic functions. Since there are thousands of other cryptocurrencies, it is difficult to say if all of them perform these functions; therefore, this chapter concentrates mostly on Bitcoin, as it is the most well-known cryptocurrency.

4.1 Medium of exchange

Considering cryptocurrencies have the ability to be used from any device with an internet connection, they can potentially serve as a medium of exchange. Nevertheless, officially fulfilling that function is one thing; generating demand to be used as a medium of exchange is another. Bitcoin has been and is still being used to purchase goods and services. However, the prices are still usually listed in US dollars rather than Bitcoin. Few stores will accept Bitcoin, and even if they do, the value will be expressed in dollars rather than Bitcoin. Dollars and other currencies are legal tender (must be accepted as payment for a debt), but cryptocurrencies like Bitcoin are not.

4.2 Unit of account

Due to changing demand and inconsistent supply, as well as the lack of an authority that can manage the supply to maintain a stable value, cryptocurrencies are now completely ineffective as a unit of account. Even those who have made a fortune trading Bitcoin disclose their net worth in dollars rather than bitcoins. The market value of Bitcoin and other cryptocurrencies is measured in dollars. Bitcoin may one day fulfil this function, but not right now.

4.3 Store of value

As discussed in the previous chapter, "store of value" refers to an item, commodity, or currency's ability to be preserved, recovered, and exchanged in the future without losing value. One of the major barriers to the adoption of cryptocurrencies as money is that the currency has demonstrated great volatility and volatile market price in

recent years, making it exceedingly dangerous as an asset for holding one's capital. The volatility may begin to flatten off as people gain a better understanding of what bitcoin is and how the fundamental technological qualities that were designed to function as a peer-to-peer payment method work. As a result, Bitcoin may be able to fulfil this job in the future, but it is not currently possible now.

CONCLUSION

Cryptocurrencies are a relatively new technology that is rapidly gaining prominence. The primary purpose of this final thesis was to summarize general information and expertise about cryptocurrencies and provide an impression of how they relate to regular money. The thesis also focuses on three separate cryptocurrencies, each of which is unique and is used in a different way, as well as having a different history of origin.

The first chapter covered general facts regarding cryptocurrencies. It focuses on the mysterious origins of Bitcoin, the world's first cryptocurrency. This chapter also includes general information regarding cryptocurrency cryptography, including how to acquire them and where to store them.

The second chapter delves into the background of each cryptocurrency, as well as what form of storage would be appropriate for someone who has recently purchased their first cryptocurrency and what they can do with it once they've decided to use it.

The third chapter’s describes what fiat money is and how they differ from commodity money. It also goes through its history and development and finally describes the definition of three functions of economy which are needed to be fulfilled in order for money to work properly in today’s world

The last chapter of thesis is focused on the three previously mentioned economic functions which are then applied to cryptocurrency in order to decide whenever they are ready or not to be fully utilized as traditional money.

Traditional money and cryptocurrencies are not the same, they differ in their functioning, acquirement, and storage. When it comes to storing money, a person doesn't have the same options because he or she doesn't store actual coins, but rather the address on which the blockchain they are kept. Cryptocurrencies are safe from hacking because they use private-public key cryptography and are untraceable. Although being untraceable is a nice quality, it can be exploited for malevolent purposes on the dark web. On the one hand, not every country accepts every cryptocurrency or wallet. On the other hand, the number of companies that support bitcoin is growing every day and purchasing items with cryptocurrency is becoming more convenient. In recent years, cryptocurrency market prices have been unpredictable, and there has been a lack of

authority to manage the supply to maintain a stable value, among other issues. Until these limitations are removed, cryptocurrencies will not be completely prepared to perform all necessary economic functions and be embraced as the money we use in everyday life.

Despite the fact that they have been there for almost a decade, they are still in their infancy and their full potential has yet to be realized. A person who decides to invest in cryptocurrencies has to understand fully how exactly cryptocurrencies work and carefully consider all the problems that come with it. In general, the only option is to wait and see what the future holds. Because in the future, new technologies and conditions may develop that cast this picture in a new light.

LITERATURE

A brief history of bitcoin & cryptocurrency. (2019). Ledger. Retrieved December 12, 2021, from https://www.ledger.com/academy/crypto/a-brief-history-on-bitcoin-cryptocurrencies

Anonymous. (n.d.). *Store of Value*. Binance Academy. Retrieved May 26, 2022, from https://academy.binance.com/en/glossary/store-of-value

Ashford, K., Curry, B. (Ed.). (2021). *What Is Bitcoin and How Does It Work?* ForbesAdvisor. Retrieved December 12, 2021, from https://www.forbes.com/advisor/investing/what-is-bitcoin/

Baldridge, R. (2021). *Why The Father of Bitcoin Is Nowhere to Be Found: In 2008, Satoshi Nakamoto appeared out of the ether to establish the world's first cryptocurrency. Then he disappeared just as abruptly*. Robb Report. Retrieved October 31, 2021, from https://robbreport.com/lifestyle/finance/bitcoin-founder-satoshi-nakamoto-1234613022/

Chapman, B. (2018). *Bitcoin: What is it, where can you use it and is it worth investing?* Independent. Retrieved December 12, 2021, from https://www.independent.co.uk/news/business/news/bitcoin-what-is-cryptocurrency-where-use-investment-dark-web-illegal-explained-value-exchange-rate-a8082491.html

Chen, J. (2022). *Fiat money*. Investopedia. Retrieved May 26, 2022, from https://www.investopedia.com/terms/f/fiatmoney.asp#:~:text=Key%20Takeaways-,Fiat%20money%20is%20a%20government%2Dissued%20currency%20that%20is%20not,U.S.%20dollar%2C%20are%20fiat%20currencies.

Conway, L. (2021). *What Is a Blockchain?* Investopedia. Retrieved November 19, 2021, from https://www.investopedia.com/terms/b/blockchain.asp

Conway, L. (2021). *Best Bitcoin Wallets*. Investopedia. Retrieved December 12, 2021, from https://www.investopedia.com/best-bitcoin-wallets-5070283

Downey, L. (2021). *Store of Value*. Investopedia. Retrieved May 26, 2022, from https://www.investopedia.com/terms/s/storeofvalue.asp#:~:text=A%20store%20of%20v

alue%20is%20essentially%20an%20asset%2C%20commodity%2C%20or,worth%20the%20same%20or%20more.

Fiat Money: *What is Fiat Money?* Corporate Finance Institute. Retrieved May 26, 2022, from https://corporatefinanceinstitute.com/resources/knowledge/economics/fiat-money-currency/

Frankenfield, J. (2021). *Dogecoin (DOGE)*. Investopedia. Retrieved December 12, 2021, from https://www.investopedia.com/terms/d/dogecoin.asp

Furneaux, N. (2018). *Investigating cryptocurrencies: understanding, extracting, and analyzing blockchain evidence*. Wiley.

How DigiCash Blew Everything. (1999). NEXTMAGAZINE. Retrieved October 31, 2021, from https://cryptome.org/jya/digicrash.htm#2

Gerstein, J. (2021). *Crypto Characters: Was David Chaum Actually the Start of the Bitcoin Movement?* CryptoVantage. Retrieved October 31, 2021, from https://www.cryptovantage.com/news/crypto-characters-was-david-chaum-actually-the-start-of-the-bitcoin-movement/

Gupta, R. (2021). *How and Where You Can Spend Dogecoin in 2021*. Martek Realist. Retrieved December 12, 2021, from https://marketrealist.com/p/dogecoin-where-to-spend/

Marr, B. (2018). *Blockchain: A Very Short History of Ethereum Everyone Should Read*. Forbes. Retrieved December 12, 2021, from https://www.forbes.com/sites/bernardmarr/2018/02/02/blockchain-a-very-short-history-of-ethereum-everyone-should-read/?sh=3fc30b2e1e89

Mehta, M. (2020). *Public Key vs Private Key: How Do They Work?* InfoSec Insights. Retrieved November 19, 2021, from https://sectigostore.com/blog/public-key-vs-private-key-how-do-they-work/

Mesk, V. (n.d.). *Unit of Accoun*t. Binance Academy. Retrieved May 26, 2022, from https://academy.binance.com/en/glossary/unit-of-account

Prypto. (2016). *Bitcoin For Dummies*. John Wiley.

What is cryptography? Retrieved October 31, 2021, from https://www.coinbase.com/learn/crypto-basics/what-is-cryptography

Solomon, M. G. (2019). *Choosing the Best Ethereum Wallet for You*. Dummies. Retrieved December 12, 2021, from https://www.dummies.com/article/business-careers-money/personal-finance/cryptocurrency/choosing-the-best-ethereum-wallet-for-you-263666

Spilka, D. (2018). *How Do I Spend My Bitcoin? (And where?)*. Kiplinger. Retrieved December 12, 2021, from https://www.kiplinger.com/investing/cryptocurrency/603697/how-do-i-spend-my-bitcoin-and-where

Thompson, B. (2021). *10 BEST Dogecoin Wallet: Store DOGE in Windows, Mobile*. Guru99. Retrieved December 12, 2021, from https://www.guru99.com/best-dogecoin-wallets.html

What Are Public and Private Keys? (2021). Cryptopedia. Retrieved November 19, 2021, from https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-what-is-public-key-cryptography

What Can I Buy with Ethereum?. Retrieved December 12, 2021, from https://www.bitrates.com/guides/ethereum/what-can-i-buy-with-ethereum

What Is Crypto Mining? Https://freemanlaw.com/. Retrieved November 19, 2021, from https://freemanlaw.com/mining-explained-a-detailed-guide-on-how-cryptocurrency-mining-works/

Wu, J. (2021). *Ethereum's History: From Zero to 2.0*. WisdomTree. Retrieved December 12, 2021, from https://www.wisdomtree.com/blog/2021-07-15/ethereums-history-from-zero-to-20

SYMBOLS AND ABBREVIATIONS

Abbreviations:

API	Application Programming Interface
BTC	Bitcoin
CPU	Central Processing Unit
DOGE	Dogecoin
ETC	Ethereum Classic
ETH	Ethereum
GPU	Graphic processing unit
ICO	Initial Coin Offering
POW	Proof-of-work
USB	Universal Serial Bus