



Ekonomická
fakulta
Faculty
of Economics

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

University of South Bohemia
Faculty of Economics
Department of Applied Mathematics and Informatics

BACHELOR THESIS

Dark Web and Cryptocurrency

Written by: Nugerbek Bolatov

Supervisor: PhDr. Marek Šulista, Ph.D.

České Budějovice 2023

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Nugerbek BOLATOV
Osobní číslo: E18098
Studijní program: B6209 Engineering and Informatics
Studijní obor: Economic Informatics
Téma práce: Dark Web and Cryptocurrency
Zadávací katedra: Katedra aplikované matematiky a informatiky

Zásady pro vypracování

The objective of the thesis is to describe basic principles of the interdependence and mutual influence of the dark web and cryptocurrency.

Metodický postup:

1. Study of selected literature
2. Definitions of dark web (why it exists and how it works) and cryptocurrency (when and how it was founded, difference between cryptocurrency and normal currency)
3. Classification of dark web and cryptocurrency (types of cryptocurrency and which are most popular, advantages of each cryptocurrency)
4. Establishing connection between dark web and cryptocurrency (cryptocurrency is used to pay for illegal activities)
5. Connection analysis (cryptocurrency is not trackable)
6. Conclusion (symbiosis – cryptocurrency allows the dark web to exist, dark web guarantees demand on cryptocurrency)

Rozsah pracovní zprávy: 40 – 50 stran
Rozsah grafických prací: dle potřeby
Forma zpracování bakalářské práce: tištěná

Seznam doporučené literatury:

1. Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. Sebastopol: O'Reilly Media, Inc.
2. Bailis, P. & Song, H. (2017). Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts: Hardware for Deep Learning. *AMC*, 60 (5).
3. Eddison, L. (2018). *Tor and The Deep Web: The Complete Guide to Stay Anonymous in The Dark Net: Two Manuscripts In one*. Kindle Edition.
4. Ozkaya, E. & Islam, R. (2019). *Inside the Dark Web*. Abingdon: Taylor & Francis Ltd.
5. Paganini, P. & Amores, R. G. (2012). *The Deep Dark Web: The Hidden World*. CreateSpace Independent Publishing Platform.
6. Rodgers, E. J. (2018). *What is the Dark Web? The Truth about the Hidden Part of the Internet*. Kindle edition.
7. Vigna, P. & Casey, M. J. (2015). *The Age of Cryptocurrency: How Bitcoin and Blockchain are Challenging the Global Economic Order*. St. Martin's Press.

Vedoucí bakalářské práce: PhDr. Marek Šulista, Ph.D.
Katedra jazyků
Konzultant bakalářské práce: doc. Ing. Ladislav Beránek, CSc.
Katedra aplikované matematiky a informatiky
Datum zadání bakalářské práce: 20. ledna 2020
Termín odevzdání bakalářské práce: 17. dubna 2021



doc. Dr. Ing. Dagmar Škodová Parmová
děkanka

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA

Studentská 13
370 05 České Budějovice

400 76 658, DIČ CZ600766565



doc. RNDr. Tomáš Mrkvička, Ph.D.
vedoucí katedry

V Českých Budějovicích dne 29. ledna 2020

Prohlašuji, že svou bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to - v nezkrácené podobě vzniklé vypuštěním vyznačených částí archivovaných Ekonomickou fakultou - elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích 14.04.2023

.....
Nugerbek Bolatov

Acknowledgment

First and foremost, I would like to thank my supervisor PhDr. Marek Šulista, Ph.D. for the guidance and valuable advice that he offered me.

I would also like to thank doc. Ing. Ladislav Beránek, CSc., MBA for being the consultant to this work.

They are the people who believed in my idea and gave me a chance to write this bachelor thesis.

Table of Contents

1. Introduction	1
2. Theoretical Framework	3
2.1 History of Internet	3
2.2 Currency and Cryptocurrency	4
2.2.1 Currency.....	4
2.2.2 Cryptocurrencies: the “Debut” of Blockchain Technology	9
2.2.3 Cryptocurrencies: Ways of Legitimation.....	16
2.3 Deep and Dark web.....	21
2.3.1 Dark Web: History and Terminology	21
2.3.2. Cicada 3301	25
3. Objectives and Methodology	27
4. Establishing a Connection Between Cryptocurrencies and the Dark Web.....	28
5. Analysis and Conclusion.....	37
Bibliography	38
List of pictures.....	40

1. Introduction

Over the past two decades, the Internet has become an integral part of human life and a new (convenient and efficient) communication tool in society. Without a doubt, in the digital age, much of the economic, political and cultural life takes place on the Internet. The Darknet, or the Dark web, is one of the levels of the Internet.

The first level of the Internet includes a collection of indexed sites, the users of which can be identified based on the IP address. The second level, the Deep Internet, or the Deep web, is a collection of non-indexed Internet pages that cannot be found by search engines, but whose users can be identified. A distinctive feature of the Darknet is that its users, thanks to the browser and the encryption system, retain their anonymity and cannot be identified.

This technology of preserving the privacy of users is in itself neutral, but it can be used both for the benefit - for the development of creative forms of communication, and for socially dangerous acts - drug trafficking, posting pornographic content, selling weapons, searching for hitmen for hire, violation of rights for intellectual property, virtual currency, etc.

The 21st century, which, according to a number of prominent authors (Hausman 2012), was to become a "golden age" for the world economy and for economic science itself, brought severe tests to society and posed new difficult questions for scientists. Financial globalization has not met expectations. The growth of cash flows from rich countries to poor countries did not lead to an improvement in the welfare of the latter, but only to a change in the owners of their national property in exchange for fictitious capital. The global crisis provokes the acceleration of the centralization of world capital and the growth of social stratification, as well as the loss of trust in the global financial system from the perspective of population. A peculiar feature of these sentiments was summed up in the last report of the Club of Rome, the authors of which directly called for a revision of the existing economic paradigm and a change in the vector of development of society (Von Weizsäcker & Wijkman 2018).

New hopes are associated with the explosive development of digital technologies and their penetration into all spheres of public life (so-called digitalization), including the economy. Research on artificial intelligence and big data technologies, blockchain and

cryptocurrencies is especially relevant today, as they are seen as the forerunners of a new economic formation, which is called the digital, or virtual, economy.

Against the background of crisis processes and loss of confidence in traditional economic institutions, interest in cryptocurrencies is growing; this topic is especially popular today both among the scientific community and the general public. Sometimes they even see them as "digital gold", the latest stage in the digital evolution of money, a miniature model of a "virtual" economy (Swan 2015).

A large amount of literature is published on the topic of blockchain and cryptocurrencies, but most of it is not directly scientific in nature and is published in open access in the form of essays or quasi-scientific notes by representatives of the digital elite - the digerati. Using this example, one can trace the change in the process of producing scientific knowledge in the areas related to new digital technologies of the 21st century. Nevertheless, I would like to note the works of N. Popper (2015), D. Tapscott and A. Tapscott (2016), which investigate the changes that cryptocurrencies and blockchain will bring to the economy and society as a whole. In other works, for example by A. Antonopoulos (2014), the technical side of the issue is revealed.

The aim of this thesis is to understand the principle of the interdependence and mutual influence of the Dark web and cryptocurrency. In order to do this, it is important to first provide a brief description of cryptocurrencies and the underlying blockchain technology, as well as analyze their evolution and the reasons why they managed to gain a foothold in the modern financial system in one way or another.

2. Theoretical Framework

2.1 History of the Internet

The world's first Internet was born with the creation of a research computer network called ARPANET. Its main task was packet switching of the US Department of Defense Advanced Research Projects Agency. A prerequisite for the creation of such a network was the launch of an artificial Earth satellite in the USSR in 1957. After this event, in order to increase the degree of information security in case of war, the United States Department of Defense urgently ordered the development of a reliable system for data transmission and allocated the necessary funds for this. A special agency DAPRA, which was responsible for the introduction of new technologies in the United States, took up the issue of creating a computer network. Over time, ARPANET has evolved and become in demand by scientists from various fields of science.

An attempt was made to establish the first network connection on October 29, 1969. Charley Kline of the University of California (Los Angeles) tried to connect remotely to a PC located 640 km away at the Stanford Research Institute, where Bill Duvall confirmed the successful broadcast of each character over the telephone. However, out of five characters of the word "LOGON", which was a special authorization command in the system, on the first attempt it was possible to transmit only the first three characters - "LOG", after which a failure occurred in the network. However, after the return of APRANET to operational status a few hours later, the next attempt by scientists to establish communication at a distance was crowned with success. The date 10/22/1969 can rightfully be considered the date of the appearance of the world's first Internet.

The first program for the exchange of e-mails on the Global Network appeared in 1971 and immediately became in demand among Internet users. In 1984, a computerized domain name distribution system began to function, which made it possible to obtain information about a site area on the Web.

In addition, in 1984, another large-scale network, NSFNET, appeared, which was created by the United States National Science Foundation. It included many small networks, including the then popular Bitnet and Usenet, and had significantly higher bandwidth compared to the ARPANET network. Thus, the latter acquired a serious competitor. More than 10,000 PCs were connected to NSFNET in less than a year, and this network has gradually become associated with the word "Internet".

The creation of the IRC - Internet Relay Chat protocol laid the foundation for the first chat, which provided real-time communication between users. This happened in 1988.

However, the global network did not become the main provider of data until 1995, when its traffic exceeded the volume of transmitted information of the popular file transfer protocol FTP. This was the impetus for the creation of the W3C - the World Wide Web Consortium. It is worth noting that it was the latter that gave the appearance of the previously faceless Internet. Thus, since 1996, the terms "Internet" and "World Wide Web" almost completely replace each other (Ryan 2013).

2.2 Currency and cryptocurrency

2.2.1 Currency

What is a Currency?

Currency is the main means of payment in the modern world. Money in itself has no real value: a piece of metal or a sheet of paper gets its value only if some person is willing to exchange some good for them. Without understanding the functions of the currency, the formation of its exchange rate, it is impossible to accumulate and increase funds in the long term.

Second definition: money in the form of paper or coins, usually issued by the government and accepted at face value as payment. However, in recent years, a new concept has come into use: virtual currency. This is money that has no physical form or government backing. Regulation and control rests with the developer (Frankenfield 2022).

The History of the Appearance of Currency

Initially, the only possible method of making trade transactions was barter. But in international trade, the barter system has shown its inefficiency.

First, it is difficult to find a buyer in advance who is ready to offer something the seller needs. Secondly, even large trading caravans were not always able to deliver all the bartered goods to their destination. Within each country, their own primitive money was

created (cowry shells, bronze mini-copies of weapons, coins). But such "means of calculation" were of value only to one community.

According to the book by Jonathan Williams "Money. A History" (1997), the first prototype of an international currency appeared long before the advent of our era. It is known that international trade between Egypt and Mesopotamia was not carried out according to the barter system. Gold and silver items, including jewelry, were used as a universal medium of exchange.

The value of precious metals was recognized in both countries. Of course, the use of jewelry and everyday items instead of money made the transaction difficult, leading to the need to check the weight and quality. But it was precisely such a system that gave the prerequisites for the emergence of standardized ingots.

Almost until the end of the 19th century, international trade was based on money made from gold. Most of the nation's money was essentially just different ways of measuring the weight of the precious metal. Not only merchants, but also travelers carried gold jewelry and ingots with them, knowing that such a currency would be accepted in almost any country in Europe and the Middle East.

During the Bretton Woods Conference of 1944, exchange rates throughout the world were pegged to the US dollar (which could be exchanged for a fixed amount of gold). In the 1950s, most national currencies were not freely convertible, and fixing the exchange rate made it relatively easy to manage the Bretton Woods system.

By the beginning of the 1970s, the world had changed dramatically: the volume of international trade increased, governments of states tried to minimize the economic consequences of the war by issuing money. Virtually worldwide inflation led to the fall of the Bretton Woods system in 1978 and its replacement by the Jamaican Accords.

Now the market has flexible exchange rates, which are formed on the basis of supply and demand. In addition to US dollars, international currencies include the English pound, Chinese yuan, euro and Japanese yen.

Types of Currencies

The classification of currencies is carried out according to many features and criteria. It is impossible to single out certain types of currencies. For example, according to ownership, the currency can be national, foreign and collective. According to the degree of circulation, the following types of currency are distinguished:

- convertible;
- partially convertible;
- non-convertible.

The first variety can be easily exchanged for another currency. With the second category, this is also possible, but with certain difficulties. In the third case, the national currency is used only within the issuing country. Usually distinguished are the most expensive currency in the world and the most stable. These categories almost never overlap.

Types of International Currencies

It is conditionally possible to single out the types of international currencies that are used in a number of countries as the main payment unit. The American dollar and the euro can be safely attributed to this category.

Despite the fact that these monetary units are gradually losing their stability, their rate is increasingly dependent on the external economic situation in the world, the main calculations are made in dollars and euros. Prices for large goods in our country are also, one way or another, tied to the dollar. If you are going to buy real estate or vehicles in the foreseeable future, it is better to collect money for these purposes in foreign currency.

New Type of Currency

A new type of currency appears regularly on the world market. Today, electronic money can be attributed to this category. Now the currency does not have to be paper or metal. With the spread of plastic bank credit cards, we increasingly refuse to cash out money, because you can pay with a card in a store, pay for purchases on the Internet. it is possible that in a few decades all countries of the world will refuse to issue money, because

their printing and minting requires a lot of money. The cost of electronic currency is much less.

Main Types of Currency

The world uses the main types of currencies that have high liquidity. They can be easily exchanged for another currency at a favorable rate. For comparison, if you have US dollars on hand, you can go to any bank and make an exchange. If you have Japanese yen or Swiss francs, despite their high level of stability, you will not be able to quickly exchange currency.

Types of Currencies According to their Influence on the World Economy

The classification of currencies carries a specific semantic load, characterizes it from a certain point of view, depending on the criterion or attribute being classified. Thus, the types of currencies in terms of their influence on the world economy reflect the external economic situation in the world. Weakness, strength of the monetary unit depends on the stability of its exchange rate to other currencies of the world, the nominal value, and the provision of gold and foreign exchange reserves. The most stable currencies in the world include the Swiss franc, the British pound. The strongest currency is the euro and the US dollar.

To create foreign exchange reserves, national banks use the Australian, the American, the Canadian dollars, the Swiss franc, the British pound, the Japanese yen and the euro as a reserve currency. A change in the exchange rate of any reserve currency affects the economic growth rate of most countries in the world.

Relationship Between the Standard of Living and the Price of a Currency

The connection between the standard of living and the price of the currency is the impact of inflationary processes on people's livelihoods: the faster money depreciates in the country, the more the population suffers. The degree of change in the quality of life depends on the stage of inflation development (Ullman 2022):

- The first stage contributes to a decrease in the income of persons with a fixed income (pensions, allowances, scholarships, etc.).
- The second stage affects wages, as they rise more slowly than prices. As a result, the labor force moves to profitable sectors of the economy to maintain the same standard of living. Small and medium-sized firms also suffer, as inflation "eats" their working capital.
- The third stage affects the state. To finance the increased spending, the state starts issuing money, but the growing supply of money increases the rate of depreciation of the currency.

Business owners can earn income if the price of the finished product rises faster than the price of inputs.

Currency Functions

The role, the economic essence of the currency is reflected in its functions.

Currency functions:

- a measure of the value of all goods;
- means of circulation between buyers, sellers;
- a store of value as the most liquid property;
- a means of payment for services, goods, various financial obligations (wages, loans, taxes, rent of land, housing, etc.).

In international trade relations, the currency performs the function of world money: it acts as a common equivalent in the process of economic relations of all countries.

Special Types of Currencies

Special types of currencies are intended for state mutual settlements exclusively in a non-cash form. In world practice, there are clearing currencies and the currency of the IMF (International Monetary Fund).

Clearing currencies are designed for use in international trade transactions. When concluding payment agreements, the participating countries determine the type of clearing currency for mutual settlements under the concluded trade agreement. The IMF special currency (Special Drawing Rights) is a means of payment used by countries to equalize the parity of exchange rates (foreign exchange interventions) by replenishing reserve assets.

Reserve Currencies

Reserve currencies are generally accepted national currencies in the world, intended for the accumulation of foreign exchange reserves by central banks. Performing the function of an investment asset, the reserve currency serves as a way to form the currency parity. It is used, when necessary, as a means of payment in foreign trade transactions by other countries.

The state, whose currency is considered a reserve, has advantages in covering the deficit of the balance of payments with its own national currency, strengthening the country's corporations in the international market. Since 1944, after the Bretton Woods agreement, the role of the reserve currency has been played by the US dollar. World systems use it to form the level of international prices for a particular product, to build all the statistics.

2.2.2 Cryptocurrencies: the “Debut” of Blockchain Technology

A cryptocurrency is a medium of exchange that is digital, encrypted and decentralized. Unlike the U.S. Dollar or the Euro, there is no central authority that manages and maintains the value of a cryptocurrency. Instead, these tasks are broadly distributed among a cryptocurrency's users via the internet (Ashford & Schmidt, 2022). Examples of such cryptocurrencies are Bitcoin, Ethereum, Litecoin, Zcash, Dash, Monero, and many others. Their developers are programmers from all over the world. The technological principle of

the functioning of cryptocurrencies is the blockchain. Blockchain is a cryptographically encrypted distributed registry in the form of sequentially chained blocks that store information about the history of transactions in a peer-to-peer network. Historically, the first blockchain project was the Bitcoin cryptocurrency, created by a programmer/team of programmers under the pseudonym Satoshi Nakamoto in 2008.

As conceived by the creators, in order to use the Bitcoin cryptocurrency, it is enough to install the client program and create an account to which the electronic wallet will be linked. After that, any owner of a laptop/smartphone with Internet access will be able to exchange payment units with other users of the Bitcoin network without intermediaries. An important circumstance is that the trust mechanism in this peer-to-peer network is provided by built-in algorithms, the operation of which was supported by the network participants themselves. This is what, according to the plans of the developers, will allow people to literally go beyond the existing financial system and freely dispose of their funds themselves. Let's take a closer look at how blockchain technology and other solutions make this situation possible.

As mentioned, a distinctive feature of most cryptocurrencies, and in particular Bitcoin, is their decentralization: the chain of transactions is not stored in one place, but in the wallets of all participants. In addition, it is stored in encrypted form, which protects it from hacking and modification (security). All operations necessary for the functioning of the network are performed in the electronic environment by various devices, depending on the mechanism of operation of a particular blockchain/cryptocurrency (for example, video cards, processors). In addition, the blockchain chain cannot be changed in the absence of a consensus decision of the network participants. Finally, cryptocurrencies are open and at the same time pseudonymous (in rare cases anonymous) systems. This means that information about transactions between participants is available online, but information about the participants themselves is hidden (Mainelli & Smith, 2015).

Mining is important for understanding the phenomenon of cryptocurrencies — the activity of maintaining a distributed platform and creating new blocks with the ability to receive rewards in the form of emitted currency and/or commission fees. Miners perform computations to carry out transactions by cryptographically encrypting new blocks, and rewards incentivize people to expend their computing power and thereby keep networks running. Thus, two goals are pursued: 1) "monetary" emission; 2) creation of new blocks.

There are two main mining mechanisms: Proof-of-Work and Proof-of-Stake. In the first case, the miner with the highest computing power has the greatest chance to encrypt a new block and receive a reward, in the second case, the miner with the largest cryptocurrency balance.

The mining mechanism allows to avoid inflation: the creators of cryptocurrencies can limit the speed of creating new blocks (that is, the frequency of emission), as well as the reward for their creation (that is, the volume of emission). For example, the Bitcoin blockchain is formed every 10 minutes. In addition, every 4 years, the reward for the found block of the chain is reduced: initially it was 50 BTC, since 2012 - 25 BTC, since 2016 - 12.5 BTC. Finally, the Bitcoin system has a built-in limit on the maximum number of coins: 21 million.

Let's give an example of how a public blockchain works as a payment system: two network users agree to carry out a transaction (for example, cryptocurrency in exchange for pizza). The sender of the payment indicates the address of the recipient's wallet, the amount of the transfer, and, if necessary, other information. The transaction is verified simultaneously by his private key as well as the public key, after which it is combined with other transactions that are being carried out at the same time. This array of information is cryptographically encrypted (hashed) by the miners and ends up in a new block that continues the chain. All participants (network nodes) update their versions of the blockchain and confirm that the block is formed according to the rules. If the block is formed incorrectly as a result of unauthorized interference or due to data transmission errors, then the nodes will not include it in the chain and the transaction is not executed. After that, the specified amount is transferred to the seller's wallet, and the transaction is considered completed.

Cryptocurrency: Types and their Features.

Cryptocurrencies can be roughly divided into three main types: Bitcoin, altcoins (including stablecoins) and tokens, which in turn include DeFi tokens. Each of these groups has its own characteristics.

Despite the fact that Bitcoin and altcoins are types of cryptocurrencies, they are not money in the usual sense. They are a complex digital product with their own crypto code and encrypted record.

To become money, they go through a complex process of transformation and processing using special technologies. Let's take a closer look at the different types of cryptocurrencies, their features and differences from each other.

What is Bitcoin?

The first and still leading cryptocurrency is Bitcoin. It is a global decentralized electronic payment system that allows users to make transactions among themselves without the involvement of intermediaries such as banks or other financial institutions. Bitcoin is often seen as a digital replacement for fiat currencies and gold, and still remains the number one crypto by market capitalization.



Figure 1. Bitcoin's Price History. Retrieved from <https://coinmarketcap.com/currencies/bitcoin/>

What is an Altcoin?

Altcoins, which were created after Bitcoin, represent all cryptocurrencies except the first cryptocurrency, their share in the cryptocurrency market in 2023 is about 40%. The launch of Bitcoin in 2008 and its source code became the starting point for the creation of thousands of other cryptocurrencies, which became known as alternative coins to Bitcoin, or altcoins.

Some of them are very similar to Bitcoin. For example, Charlie Lee, the creator of Litecoin, called his cryptocurrency an analogue of Bitcoin. Litecoin is a peer-to-peer currency and global payment network.

Some altcoins have goals that are different from those of Bitcoin. For example, Ethereum is the world's first programmable blockchain platform that allows developers to create and deploy decentralized applications (DApps) and smart contracts.

The IOTA cryptocurrency was created with the goal of becoming a new level of data transfer and transaction settlement for the Internet of Things (IoT) and the machine economy (machine-to-machine or M2M). IOTA uses its own proprietary distributed ledger technology, The Tangle.

Like Bitcoin, all altcoins can operate independently on their own networks using distributed ledger technology (DLT) (Capital.com Research Team, 2019). Blockchain is the most common and well-known type of DLT, however, each altcoin is unique due to its variation on the underlying code of each protocol.

What is a Stablecoin?

Stablecoins are cryptocurrencies whose exchange rate is supported by certain assets, such as strong fiat currencies (US dollar, euro, etc.), commodities (such as gold), or other cryptocurrencies, which reduces price fluctuations. In 2023, Tether and Binance USD became the most popular stablecoins. However, some stablecoins do not have a backing, for example, the Carbon and Havven coins are regulated by issuing or burning assets.

What is a Token?

All cryptocurrencies have a common goal - to speed up and simplify the process of conducting transactions. This is achieved through the use of blockchain technology, which stores all transaction information in encrypted form.

Tokens are a separate type of cryptocurrencies that do not use blockchain. Instead, they are recorded in a distributed information system of transaction blocks, which confirm the ownership of the rights to certain objects of civil rights by the owner of the digital token.

Simply put, tokens are units of account with the ability to replace financial assets (such as securities, indices, commodities, gold, etc.) in the digital world. They are digital

receipts from the creator of the token, obliging him to provide certain objects to the owner of the token.

Unlike Bitcoin and altcoins, tokens cannot function autonomously, so they are placed on top of a created crypto-network (usually ethereum and blockchain) and managed through smart contracts. Access to tokens usually requires the use of special software.

There are several types of tokens, including:

- capital tokens — securities (shares) of the company;
- utility tokens - used by online platforms and can represent points, in-game currency, reputation, etc.;
- asset-backed tokens are a kind of liability for services or goods (“Main Types of Cryptocurrencies. Coins and Tokens”, n.d.).

The last type is the most interesting. The ability of tokens to represent virtually any asset has given cryptocurrency investors access to the world of traditional financial instruments.

Tokenized versions of stocks, commodities, fiat currencies, other cryptocurrencies, property, and more have revolutionized the world of finance. Thus, tokens open up new investment opportunities and can be of significant value to investors.

Who Launches Tokens

According to CoinMarketCap, there are currently around 1,500 tokens deployed on the blockchain platforms of 24 cryptocurrencies. The largest number of tokens are deployed on the Ethereum platform. More than half of the top 100 cryptocurrencies by capitalization are Ethereum-based tokens such as Huobi (HT), Binance Coin (BNB), USD Coin (USDC) and Uniswap (UNI) .

Tether (USDT), the leading stablecoin, was released on the Omni Layer platform along with three other tokens. NEO, a platform for smart contracts and DApps, has released the NEO token, which used to be considered a Chinese competitor to Ethereum. TRON, the leading platform for DApps, has many tokens deployed on it, including BitTorrent Token (BTT), which can be used for faster downloads over the BitTorrent file sharing protocol.

What are DeFi Tokens?

Considering the various types of cryptocurrencies, one cannot fail to mention DeFi tokens, which have become especially popular among investors recently.

DeFi projects are decentralized financial platforms that offer exchanges, wallets, lending services, and other tools for financial transactions. There is a real boom in this area, comparable to the ICO in 2017.

One of the key features of DeFi projects is that developers do not have access to user funds, and all transactions take place directly between users. Recently, DeFi platforms have begun issuing their tokens, causing their prices to explode. For example, after the launch of the YFI token, issued by the DeFi platform yEarn Finance on July 18, 2021, its price rose from \$35 to \$4,800 by July 25 and to \$13,533 by October 22 of the same year.

Some DeFi tokens can rise thousands of percent per day, which can eventually lead to a bubble. It is not yet clear when this bubble will burst.

What is a Cryptocurrency Fork?

When discussing different types of cryptocurrencies according to the method of their creation, it is impossible not to mention forks. Many of the popular cryptocurrencies such as Litecoin, BCH and others are forks of Bitcoin.

A fork is a modified copy of a cryptocurrency. There are two types of forks: soft forks and hard forks. A soft fork is a soft modification of a cryptocurrency, when the changes made are reversible and do not violate its main protocol. A hard fork is a hard modification of a cryptocurrency, when the changes contradict its main protocol, and the network is divided into two parts that cannot interact with each other.

2.2.3 Cryptocurrencies: Ways of Legitimation

Today, the question of whether cryptocurrencies, and in particular Bitcoin, can be considered “full-fledged” money is practically not present, however, opponents and supporters speak of them in a completely different tone: some argue that this is nothing more than a money surrogate or even a financial pyramid; while the others, on the contrary, consider them something better than traditional government-issued fiat money. One thing is certain: a certain public consensus has formed around cryptocurrencies about the possibility of using them (as a means of exchange and as a means of investment), as a result of which they have taken their place in the financial system.

History knows examples of “private” money: the American philosopher of science and economist D. McCloskey, speaking about cryptocurrencies, gives an example of Northern Michigan banknotes that were in circulation during the so-called era of free banking, in the 1830s–1850s, in the United States, when the monopoly of public money was called into question. Nevertheless, there are no cases of successful functioning of such decentralized money in the modern sense. What factors allowed cryptocurrencies to do this?

1. Technology platform. Indeed, cryptocurrencies are very different from money in the modern sense, primarily in the mechanism of providing trust. In traditional national monetary systems, this is the responsibility of the existing legislation, one way or another controlled by the ruling power, centralized emission and the power of state coercion. Blockchain as a technology allows to create trust in an initially "untrusted" environment by executing a strict algorithm embedded in the system. The advantages described above - security, immutability, openness and pseudonymity - allow strangers to safely exchange cryptocurrencies, and also significantly reduce the cost of ensuring public consensus. This ensured the legitimization of the use of cryptocurrencies (namely Bitcoin) at an early stage of evolution in the absence of state legalization of their circulation.

One can draw an analogy with rai stones - large limestone discs mined on some islands of Micronesia (Palau, Guam) and circulated as a means of payment (Mankiw 2004). Due to their special properties and difficulties in extraction and manufacture, they ruled out the possibility of forgery, circulated only thanks to public consensus, and even had transfer records on themselves, certifying the transfer from one owner to another. The absence of a central authority regulating the issuance of rai adds to this exotic metaphor.

2. Distrust of existing financial institutions. Initially, Bitcoin was born on a wave of disillusionment with modern capitalism after the 2008 global financial crisis and spread like a viral idea among programmers and other digerati people. The first significant rise in the price of Bitcoin coincided with the banking crisis in Cyprus in 2012-2013, and further growth in their exchange rate more than once coincided with financial shocks (Extance 2015). This is consistent with the original intention of the creators of Bitcoin: to make not just a new currency, but an alternative to the entire existing monetary system.

The French postmodern philosopher Jean-Francois Lyotard characterized such situations of loss of trust as a "crisis of metanarratives" (Lyotard 1998). According to his understanding, micronarratives, not being directly associated with power mechanisms, ensure the integrity of everyday life experience at the level of individuals and social cells, and metanarratives provide legitimization of some existing order in general and central public institutions in particular. Lyotard pointed to the crisis of such metanarratives as the emancipation of the worker and the growth of social wealth as a result of the ever-deepening division of property between employees and owners of capital. The crisis of dominant metanarratives leads to the possibility of the emergence of new competing narratives (or a wider distribution of existing micro- and meso-narratives) with their subsequent fixation in the public consciousness. In this case, we come to the interpretation of cryptocurrencies as the next stage in the evolution of money or as an alternative "narrative" of exchange and the world economy as a whole.

Economist and philosopher Mark Fisher came to similar conclusions. In his opinion, capitalist realism is a kind of Deleuzian "dark potentiality", "an unnamable Thing", implicitly mediating all the processes taking place in society and all existing phenomena: science, religion, culture; everything is passed through the sieve of capitalism, everything is assigned a monetary (market) value, everything is bought and sold. According to the author, the global financial crisis of 2008 did not undermine capitalist realism as such, but "discredited it in every sense of the word" (Fisher 2010). The general public has lost confidence in such a system of "financialism" (situations of merging financial and industrial capital and their concentration in the hands of a limited group of people), and this gave rise to new searches for alternative options for organizing economic life, one of which was cryptocurrencies.

3. Cryptocurrencies as a cultural phenomenon – a meme. At the beginning of their evolution, cryptocurrencies acted not only as an economic object, but as a kind of symbol,

idea, meme. The term "meme" was introduced by the biologist and philosopher of science R. Dawkins. Initially, these are units of information that circulate and are consistently reproduced in culture (Dawkins 2016). Cryptocurrencies exploit the ideas of getting rich quick, globalization up to anti-statehood, the dominance of mathematics and the free circulation of capital. Subject, according to Dawkins, to the laws of natural selection, cryptocurrency as a meme has been remarkably successful, especially in the digital environment, which has allowed the formation of a community of "crypto enthusiasts" - people from all over the world who believe that, regardless of the state of the existing financial system, cryptocurrencies will sooner or later replace conventional money and will literally become the "currency of the future", "digital gold".

This group of people, who were the first to start using cryptocurrencies, not only provided demand for them, but also significantly supported them in the media space: the topic began to be widely discussed, and the circle of people familiar with it was constantly expanding.

4. Demand from the shadow business. Already in the early years of its existence, the pseudonymity of Bitcoin and the difficulty in tracking its transactions began to attract various illegal structures. This contributed to the creation of a negative aura around cryptocurrencies in the public mind and even led to serious debate about the need for a complete ban. While the FBI (according to their own claims) has already learned how to track transactions using Bitcoin, there are a number of other currencies (Monero, Zcash) that provide complete anonymity to their users if necessary.

It was various shadow structures, along with the first crypto enthusiasts, that created the demand for Bitcoin when it had not yet attracted wide public attention. In 2011, the American William Ross Ulbricht organized a criminal community and created an anonymous online trading platform, where payments between participants were made in cryptocurrency. The project was called the Silk Road and made it possible to illegally acquire goods prohibited in many countries: drugs, weapons, counterfeit money, pornography and much more. According to the FBI, the site's annual turnover was up to \$15 million; over 3 years of its existence, more than 1 million transactions worth more than 9.5 million Bitcoins were carried out. In 2013, after a special operation by the FBI, the Silk Road was liquidated, and Ulbricht was arrested and received two life sentences.

Another class of players that cryptocurrency attracted by their lack of state control, cross-border and anonymity were various illegal entrepreneurs and corrupt officials who found an easy way to legalize their income in Bitcoin. The greatest demand arose in China, where the fight against corruption is particularly active, as well as in the CIS countries.

5. Financial speculation. The idea of “easy” earnings that underlies cryptocurrencies has attracted not only miners to the cryptocurrency ecosystem. Financial speculators have found a new space in cryptocurrencies to inject fictitious capital and extract exchange rate profits. Fictitious capital is capital that has its own movement, different from the circulation of real capital, both in production and in monetary forms, and is an instrument for redistributing generated income or accumulated wealth.

With the growing popularity of cryptocurrency exchanges, part of the capital circulating on stock exchanges began to flow into cryptocurrencies, causing an explosive growth in their rate: in a few years, quotes have grown dozens of times. However, unlike the factors listed above (even if illegal), this factor has generated inorganic demand associated only with short-term plans of stock market players to extract high speculative income.

For example, the rise in Bitcoin market capitalization in 2017 outpaced not only the rise in US stock prices before the 2008 global financial crisis, but also the textbook pyramid schemes of the 18th century: the bubble of the Mississippi Company (1720) and the South Sea Company bubble (1723) (Domm 2017). This not only devalues the ideas of crypto enthusiasts, but also prevents the cryptocurrency from functioning as a means of payment. Against the backdrop of speculative hype, the Bitcoin network experienced an unprecedented heavy load at the end of 2017, when the price hit an all-time high, coming close to \$20,000 per Bitcoin. This led to a significant increase in transaction processing time and a multiple increase in miner fees. The network was overloaded with unprocessed payments, and the miners did not have time to process them in a timely manner: the network was paralyzed. At the beginning of 2018, this rally ended with a sharp drop in the value of cryptocurrencies by 60-70% in a few days.

Thus, the dream of cryptocurrencies as “digital gold” remained unfulfilled by the end of the first decade of their existence, on the contrary, they turned into a speculative highly volatile asset. The appearance of non-deliverable futures on some American exchanges (for

example, CBOE) further exposed the essence of the ongoing “derivatization” of this process.

6. Creation of a regulatory framework for regulating the circulation of cryptocurrencies. At the initial stage, people used gaps in national legal systems, and transactions with cryptocurrencies were in the "gray" zone. Only recently, various countries have begun to develop legislative regulation of their turnover, which formally meant legalization in one status or another.

It is worth saying that there is no single approach to regulating the circulation of cryptocurrencies: it is defined both as a means of payment, and as a digital asset, and as a specific product. At the moment, the highest level of adoption of cryptocurrencies is demonstrated by three categories of countries: developed countries (Japan, EU, South Korea, USA), third world countries with a weak national currency (Zimbabwe, Venezuela), as well as post-Soviet countries (Estonia, Russia, Ukraine). Some Arab countries demonstrate the lowest level of acceptance at the state level (in particular, Saudi Arabia discusses how cryptocurrencies comply with Sharia law), as well as China, which has significantly tightened legislation on cryptocurrencies, but there is no talk of a complete ban today.

In the first case (USA/EU/Asia), the adoption of cryptocurrencies is associated with the loyal attitude of the authorities and the presence of a regulatory framework, high income and level of education of citizens who are ready for such economic experiments, as well as with the attention of some institutional investors, which at this stage allows to determine the scope of regulation of the cryptocurrency sphere. Nevertheless, in 2017, many national governments began to work out the legislative regulation of this market, and it is still difficult to say how this will affect the situation. Moreover, a number of commercial banks in major countries (Toronto-Dominion Bank in Canada, Lloyds Banking Group in England, Shinhan Bank in South Korea) have severely restricted their users' cryptocurrency transactions.

In the second case (Venezuela/Zimbabwe), it is worth talking about the inevitable flight of the population from national currencies to more reliable ones (as an alternative to the dollar), regardless of the position of the national authorities. It is also indicative that the increased demand for cryptocurrency leads to a situation where the exchange rate on informal exchange platforms in these countries turns out to be significantly higher than the

average in the world. This once again confirms the thesis about cryptocurrencies as an “alternative financial metanarrative”.

In the case of the former USSR, we are dealing with a unique combination of several factors, such as a large number of technically literate programmers, distrust of state financial mechanisms after numerous crises, and a neutral attitude of the authorities. Estonia stands apart, which previously assumed the role of the European center of digital innovation and, in accordance with this, is actively introducing cryptocurrencies and blockchain in all areas.

Despite the fact that legalization is not as important for cryptocurrencies as for fiat ones, this mechanism allowed them to move out of the "gray" zone into the "white" zone, increase demand and, as a result, market capitalization. The reverse side of the process is exchange rate fluctuations as a result of negative statements by national regulators about cryptocurrencies: for example, in September 2017, the Bitcoin rate fell by more than USD \$1,000 (25%) as a result of the Chinese regulator's statement about the temporary suspension of the largest exchanges.

2.3 Deep and Dark web

2.3.1 Dark Web: History and Terminology

The history of the Dark web dates back to 1969, when Charlie Kline, a student at the University of California, Los Angeles, types the first message and sends it between computers connected to the ARPANET, the Internet predecessor developed by the Pentagon's Defense Advanced Research Projects Agency. In just a few years, a number of isolated secret networks begin to appear next to the ARPANET. Some eventually became known as the Dark web. The ARPANET in 1969 was not built with security in mind. The rapid growth of the network has made it insecure. Due to the characteristics of digitally stored information, an attacker can intercept, violate, corrupt, use, destroy, steal, and alter digital data. Depending on the value of the information, such actions will have different consequences with varying degrees of damage.

With the advent of the modern web, probably marked by the standardization of the Internet protocol suite in 1982, the problem of storing confidential or illegal data has become more acute. Early solutions include physical "data havens" - the information

equivalent of tax havens - in the Caribbean that promise to house everything from gambling to illegal pornography.

As the Internet has become more popular, lower storage costs combined with advances in file compression have caused an explosion of activity on the Dark web as users began sharing copyrighted material. Soon, decentralized data hubs are born in peer-to-peer data transmission over the Internet, some of which, such as the so-called top sites where most illegal music and movie files occur, are password protected and known only to insiders. Others, like Napster, operate openly and provide millions of file transfers per day.

In March 2000, software developer Ian Clarke releases Freenet, a revolutionary piece of software that offers an anonymous pass on the Dark web where one can access prohibited material ranging from child pornography to instructions on how to create explosives (Kastner 2020).

In September 2002, researchers at the US Naval Research Laboratory release an early version of Tor ("The Onion Router") that hides the location and IP address of users who download software (McCormick 2013). Originally designed to protect the identities of American militants and dissidents in repressive countries like China, Tor also has another natural audience: the Dark web dwellers.

In 2010, the number of extremist sites on the Dark web reached 50,000, and terrorist forums reached over 300. The illegal sale of pirated digital content is a source of funding for terrorist operations.

To this day, the Dark web is an open issue for a large number of states, as criminals use the most important idea of the Dark web - anonymity. To understand the overall picture of the current state of the Dark web, it is necessary to understand and analyze the interpretation of this term.

The Dark web (or the Darknet) is a general term that describes parts of the Internet that are deliberately not open to public viewing or hidden networks whose architecture is superimposed on the architecture of the Internet (Bloomenthal 2021). The term originally described computers on the ARPANET that were hidden, programmed to receive messages but did not respond to or acknowledge anything, thus remaining invisible to the general network.

The Dark web now is any type of overlay network that requires some kind of authorization or tools to access. The reasons for working on the Dark Web are usually related to various functions. They can be used to commit a range of crimes, including illegal file sharing, black markets, and as a means of exchanging illegal goods or services. These are often the most popular uses of the Dark web. But they are also used for a variety of other reasons. Dark webs are often cited as a means to protect political dissidents from reprisals or to allow people to bypass censorship networks. They can help raise awareness of violations and news leaks, and help protect people from surveillance. As such, and because of the many applications of the Dark web, they are a hotly contested issue.

The "Dark web" is commonly confused with the "Deep web". The deep web refers to non-indexed sites that cannot be found. In most cases, this is because these sites are password protected. Parts of the "Dark web" are purposefully hidden from the surface of the network by additional means. The vast majority of Internet sites make up the "deep web" because they are password protected.

One common way to separate Dark webs from surface webs is through encryption. Most Dark sites use the Tor encryption tool to hide their identity. Tor allows people to hide their location as if they were in another country. Tor encrypted networks require individuals to use Tor to visit them. Thus, these users' IP addresses and other identifying information are similarly encrypted. All of this combined suggests that most people can visit sites on the Dark web if they have the proper encryption tools. But it can be incredibly difficult to determine who created these sites or who controls them. It also means that if anyone involved in the Dark web reveals their identity, it can be dangerous.

Tor uses layers and levels of encryption to secure traffic by routing it through a dense network of secure relays to anonymize it. Tor itself is not illegal software, just like torrent tools are not illegal. However, in both cases, the software is usually used to carry out illegal activities (either through the Dark web or, in the case of torrent tools, to download pirated material).

In addition to illegal buying and selling, there are other, legal reasons why one might be interested in using the Dark web. People in closed societies facing extreme censorship may use the Dark web to communicate with others outside of their society. Even people in open societies may be interested in using the Dark web, especially as

concerns about government tracking and data collection continue to grow around the world.

However, most of the activity that takes place on the Dark web is illegal. It's not hard to see why this might be the case: the Dark web offers a level of identity protection not found on the surface. Criminals looking to protect their identity to avoid detection and capture are attracted to this aspect of the Dark web (Bloomenthal 2022).

Even though the Dark web seems purely criminal in nature, there are also exciting projects, thanks to which you can find real intellectuals, masters of their craft, on the Web. The Dark web is reputed to be a favorite hangout for journalists, philosophers, dissidents and other extraordinary personalities. Some companies even look for extra-class employees here, who cannot be found by conventional methods. It has its own message boards (for example, 8chan, nntpchan), its own online marketplaces for buying various goods (for example, Alphabay, Hansa), its own blogs (for example, OnionNews, Deep Web Radio). It even has its own encyclopedia - Hidden Wiki, where you can find articles on a variety of topics, as well as links to other resource sites. The main difference between the Dark web and the Surface web is its rules of operation, or, more precisely, the absence of rules while following a certain etiquette of participation.

The best example is the well-known puzzle Cicada 3301, which in 2012 provided a lot of food for discussion about the possibilities of the Dark web and ways to reveal them, based on the principle of anonymity.

2.3.2 Cicada 3301

It all started on January 4, 2012, when a post with this picture appeared on 4chan:



Figure 2. Cicada 3301's first puzzle. Retrieved from <https://www.wnycstudios.org/podcasts/notetoself/articles/meet-teenage-codebreaker-who-helped-solve-cicada-3301-internet-puzzle>

Next to it was a text: “Hello. We are looking for highly intelligent individuals. To find them, we have devised a test. There is a message hidden in this image. Find it, and it will lead you on the road to finding us. We look forward to meeting the few that will make it all the way through. Good luck. 3301” (Hern 2014). Visitors to this site are used to the fact that hooligan statements and pornographic pictures are usually published here, so they began to actively discuss what happened. Someone decided that this was the work of the secret services, since it had previously been noticed that they were actively monitoring hacker events and forums in order to attract talented young people to their ranks. It's not hard to remember how their British colleagues during World War II posted crossword puzzles in the Daily Telegraph, recruiting employees to solve the mystery of Enigma, the Germans' portable encryption system.

One way or another, the picture was reposted on other forums - and enthusiasts took up the decoding. Someone suggested opening the cicada image in a text editor. The answer was revealed immediately: the text contained the only meaningful message: “TIBERIVS CLAVDIVS CAESAR says “lxxt>33m2mqkyv2gsq3q=w]O2ntk” (“Tiberius Claudius Caesar says...”).

It was steganography, when text was “hidden” inside the file. Tiberius Claudius was the fourth Roman emperor, some immediately realized that they needed to shift the

letters four back in an incomprehensible part of the message. The result was a website address on the Internet. So, the Caesar code was solved in the first Cicada 3301 puzzle.



Figure 3. A poster found in Warsaw shows a QR Code for a website related to the Cicada 3301 mystery. Retrieved from <https://www.npr.org/2014/01/05/259959632/the-internets-cicada-a-mystery-without-an-answer?t=1643081756420>

Subsequent Cicada 3301 puzzles covered a variety of communication media (Internet, phone, music, Linux CD boot images, digital images, paper signs) and contained references to a wide range of works of literature, poetry, and art. Searchers had to decipher, for example, the ancient cryptography used by the Maya Indians. Among the finds there were GPS coordinates of places that needed to be visited to get another clue: among them are various cities not only in the USA (Annapolis, Chino, Columbus, Fayetteville, Greenville, etc.), but also in Australia, Spain, Russia, Poland, Japan, France, South Korea.

The first series of puzzles lasted about a month, the second began a year later, the third - a year later. In 2015, there were none, and in January 2016, a new sequel appeared. However, the version that Cicada 3301 was the product of the special services remained unconfirmed. Many associated the project style with Microsoft and Google's methods of recruiting experts with creative thinking and good programming skills.

3. Objectives and Methodology

This thesis focuses on establishing a connection between the existence of the Dark web and the demand on cryptocurrencies.

The main objective:

Understand how cryptocurrencies and the Dark web exist in symbiosis.

To achieve the main objective, the following methodology has been set:

- 1) *Study of scientific literature*
- 2) *Definitions of cryptocurrency and the Dark web*
- 3) *Classification of cryptocurrency*
- 4) *Establishing a connection between cryptocurrencies and the Dark web*
- 5) *Connection analysis*
- 6) *Conclusion*

This work consists of two parts: theory and analysis. In the theoretical part, the history of the Internet, the definitions of cryptocurrency and the Dark web are given. Moreover, types of cryptocurrencies, their advantages and disadvantages are discussed. Furthermore, the principles and work mechanism of the Dark web are explained.

In the analysis part, all the information from the theoretical part is analyzed and used to establish a connection between cryptocurrencies and the Dark web. It explains how cryptocurrencies allow the Dark web to exist for their anonymity and impunity, while the Dark web guarantees demand on cryptocurrencies, thus existing in symbiosis.

4. Establishing a Connection Between Cryptocurrencies and the Dark Web

Cryptocurrencies and the Darknet - What is the Relationship Between Them?

Bitcoin and other cryptocurrencies are becoming more and more popular every year. Digital assets are used in many areas of activity, including acting as the main method of payment for goods on the Dark web.

The so-called Dark side of the crypto asset economy is really the part of the iceberg that is not visible on the surface. The activity of digital coins on exchanges and a few stores is a very small part of the use of tokens. The main and most expensive transactions go unnoticed by most users - on the Dark web.

This became possible due to the main quality of the cryptocurrencies offered on the market - their anonymity and security of transactions. For this, digital assets are valued not only by hackers, but also by scammers with scammers who want to remain in the shadows during dubious trading operations with clients.

Why is Bitcoin Associated with Illegal Activity?

All criminals usually adapt to innovative technologies faster than ordinary citizens. The point is not only in the adventurism that is characteristic of them, but also due to the fact that they always strive to be ahead of representatives of law enforcement agencies who can shut them down. In this regard, settlements on the Darknet, in the market with illegal goods, have become a real and popular way to use BTC.

At one time, the Silk Road allowed people to learn about Bitcoin far beyond the cryptocurrency community. Along with the first rise in the coin rate, BTC gained a reputation as an asset for drug dealers and other criminals.

Until now, community users are facing constant accusations that BTC is used only for criminal purposes. In fact, the offshore system is more suitable for financing terrorist activities and money laundering, rather than an anonymous decentralized network through which payments pass. Pavel Durov, the creator of the VK and Telegram networks, gave a

very good answer to the proposals to ban Bitcoin and altcoins. He, at one time, proposed to ban words, because terrorists use them to communicate.

Undoubtedly, BTC brought the Dark web economy to a new level on the Silk Road, but in recent years, marketplaces on the Dark web began to cease operations one after another. What causes the extinction of a profitable but illegal business, and how closely are cryptocurrencies related to the Darknet?

Cryptocurrencies and the Dark Side of the Global Network

Digital coins, especially Bitcoin, are very popular on many DarkNet services. They act as the main payment instrument, as site users strive to achieve maximum anonymity and try to perform uncontrolled transactions. One of the first to use digital coins was sellers of illegal substances and preparations, weapons and other illegal goods.

It is impossible to access sites on the Dark web in the usual way, that is, through the classic browser that you are used to using, you are unlikely to get here. To immerse yourself in the Dark part of the global network, you will need special software, for example, the TOR browser or similar software. The emergence of cryptocurrencies has given a new lease of life to black markets online. Anonymous transactions and the very idea of decentralization made it possible to limit control by the secret services.

Are Transactions with Bitcoin Completely Anonymous?

It is no coincidence that experts prefer to use the term “pseudo-anonymity” in relation to BTC. The closest analogue is the pseudonym of an artist, actor or writer. Until a direct connection is established between a specific person and a crypto wallet, its user is anonymous. But is it possible to 100% avoid the risk of "exposure"? It turned out that there are ways to identify the owner of a cryptocurrency account.

Moreover, if you do not take special steps to hide your identity, then finding you is quite simple. For example, when buying coins in an exchanger, you need to make a transaction from a fiat wallet (bank card). Thus, the owners of the exchanger know their customers "by sight".

A similar situation occurs when making purchases in online stores. Yes, you can pay with BTC from your crypto wallet. But then you will need to give the delivery address, and this is a direct and strong thread to identify the buyer. These are just the most obvious examples. However, the bottom line is that almost every transaction with cryptocurrency, like a transaction with fiat, leaves a financial footprint.

Ross Ulbricht and the Silk Road — the Story of a Critical Mistake

In 2011, an American, Ross Ulbricht, opened an online store on the Dark web, which very quickly gained unprecedented proportions. Those who wanted to buy heroin or a fake passport applied here, and buyers could pay the bill with Bitcoin. In just 2 years, the Silk Road customer base totaled more than 1 million customers.

But at first, Ulbricht was an ordinary bookseller. At the dawn of his entrepreneurial activity, 5 employees worked in his store. At the same time, the profit of the outlet was estimated at a modest amount of \$ 10,000.

The idea of creating a criminal store arose on the basis of the concept of libertarianism supported by Ulbricht. This philosophy views taxes as coercion by the state. For the followers of this principle, cryptocurrency, due to the lack of strict mechanisms for its regulation at that time, became a real find in 2011.



Figure 4. Ross William Ulbricht. The creator of the Darknet market website “the Silk Road”. Retrieved from <https://www.wsj.com/articles/silk-road-trial-ross-ulbrichts-fate-sits-with-jurors-1423007681>

Indeed, BTC or another coin is not within the sphere of influence of state bodies. Since the mint does not issue cryptocurrencies, it was not possible to tax the flows of transactions made at that time. The result was the Silk Road, a site where you could make anonymous purchases of drugs, weapons, and other illegal goods without leaving any traces.

How was the perpetrator found? He was given an email address. In the early days of the Silk Road, Ulbricht posted it on a forum in connection with the store being created. As a result, through this address, the investigators managed to reach the owner himself and establish surveillance over him.

During the trial, Ulbricht's lawyer appealed to the fact that the FBI illegally copied personal data from a private server. During the investigation, the police found a server in Ireland at an IP address that had previously been “exposed” in the Tor network, where the Silk Road clients communicated.

The judge rejected this thesis. Activists who supported the defendant published the address of the judge on the Dark web for all to see. So, they showed the vulnerability of the personal life of every person, whoever he was. In response, the judge released personal information about those who invaded her privacy. So, the vicious circle is closed.

The creator of the Silk Road project followed some code of ethics. For example, it was forbidden to sell weapons or offer killer services on his portal, but this did not mitigate his sentence. Ulbricht was given two life sentences at once and, in addition, several more decades.

DarkMarket Takedown

150 people arrested around the world and more than 26 million euros seized as a result of a global special operation to combat smuggling on the Dark web. The law enforcement agencies of nine countries took part in Operation Dark HunTOR.

One of the largest investigations in the history of Europol, with the assistance of the US authorities, was directed against participants in illegal trading on the DarkMarket platform, which was discontinued in early 2021.

Special operations were carried out in a number of European countries, including Germany and France, as well as in Australia and the United States. 26.7 million euros (about \$31 million) in cash, digital currency and Bitcoin, 234 kilograms of drugs and 45 weapons were seized. Moreover, 67 people were arrested in the US, 47 in Germany, 24 in the UK.

Europol says many of the detainees were high-value targets. The investigation by the European law enforcement agency was a continuation of the German police raid against the DarkMarket platform, which was operated by an Australian citizen.

Moreover, the Europol press service reported that as part of the same Dark HunTOR operation, several illegal trading platforms were closed in Italy, two of which, DeepSea and Berlusconi, posted 100,000 ads for the sale of contraband products. Four administrators were arrested and 3.6 million euros in cryptocurrency were seized.

Commenting on Operation Dark HunTOR, Europol's Deputy Executive Director of Operations, Jean-Philippe Lecouffe, said: "The point of operations such as the one today is to put criminals operating on the Dark web on notice: the law enforcement community has the means and global partnerships to unmask them and hold them accountable for their illegal activities, even in areas of the Dark web" (Europol 2021).

The Koblenz prosecutor's office notes that the site was one of the largest in the world. The site had almost 500 million users and more than 2.4 thousand sellers.

- The main commodities were drugs, counterfeit money, stolen credit card details, anonymous SIM cards, and virus software.
- Trading on DarkMarket was carried out using cryptocurrency.
- In total, at least 320 thousand transactions were carried out on the site.
- The total turnover of the site is estimated at 4,650 Bitcoins and 12,800 monero. At the exchange rate at the time of the publication of the press release, this corresponded to an amount of more than €140 million.

How Does the DarkNet Work with Cryptocurrencies?

There are many Darknet networks in the world, although many people think that the DarkNet is something unified, which has no analogues. Some networks are outdated

and almost never used, but there are really popular projects. Your first visit to any Dark web might surprise you - things don't work as smoothly as you might imagine.

On the Dark web, all connections are established between trusted nodes through specific protocols and ports. All IP addresses are hidden, so it is physically impossible to enter the Darknet through such familiar browsers as Chrome or Opera.

All networks operate on the principle of decentralization and are not controlled by any management. Due to this, users get some freedom of action and security. Many sites on the "Dark side of the Internet" run on the TOR encryption protocol, which hides the identity of users and replaces their IP addresses. Also, the resource itself is hidden from prying eyes outside the DarkNet network.

How is the DarkNet Different from Other Networks?

To understand how cryptocurrencies are connected to the Dark web and how strong this connection is, you need to better understand how the network works. As it was mentioned in the theoretical part of this paper, all space on the Internet can be divided into the following groups:

- Surface web. This is a public part of the global network, the files in which are in the public domain. Users see them through simple browsers such as Chrome, Opera, Yandex, Safari and others. According to expert estimates, the visible network occupies no more than 20% of all information on the Internet.
- Deep web. These are resources that are not indexed. They do not get into search engines, and the list of Internet resources of this type includes libraries, government databases, and much more. Sites cannot be found, since the servers are not published, and a limited number of people have access to them after registration or by password.
- Darknet. This Internet space is deliberately hidden from prying eyes. Users get access through a proxy server. These resources cannot be found in search engines, and they cannot be accessed through standard browsers either.

Often people confuse the Darknet with the Deep Web, considering it to be the same space. In fact, the DarkNet is something like a network within a network that operates according to individual algorithms and protocols. It follows that cryptocurrencies for

illegal activities can be used mainly within the DarkNet. In other cases, the user will not be able to maintain absolute anonymity.

The Impact of the Darknet on Cryptocurrencies

We briefly examined the features and principles of the DarkNet network, but how does it affect the development of cryptocurrencies and their price on the market? There are many sites on the Internet that sell illegal goods, AlphaBay and Oasis stand out among them. Once these resources greatly raised the rate of some digital coins.



Figure 5. Monero's Price History. Retrieved from <https://coinmarketcap.com/currencies/monero/>

The price of Monero and Ethereum increased almost 4 times thanks to the AlphaBay and Oasis projects. It happened very simply - the management of the sites simply at some point added two tokens to the list of currencies for paying for goods. This literally exploded the value of digital assets and increased interest in them from potential buyers using the services of the AlphaBay and Oasis projects.

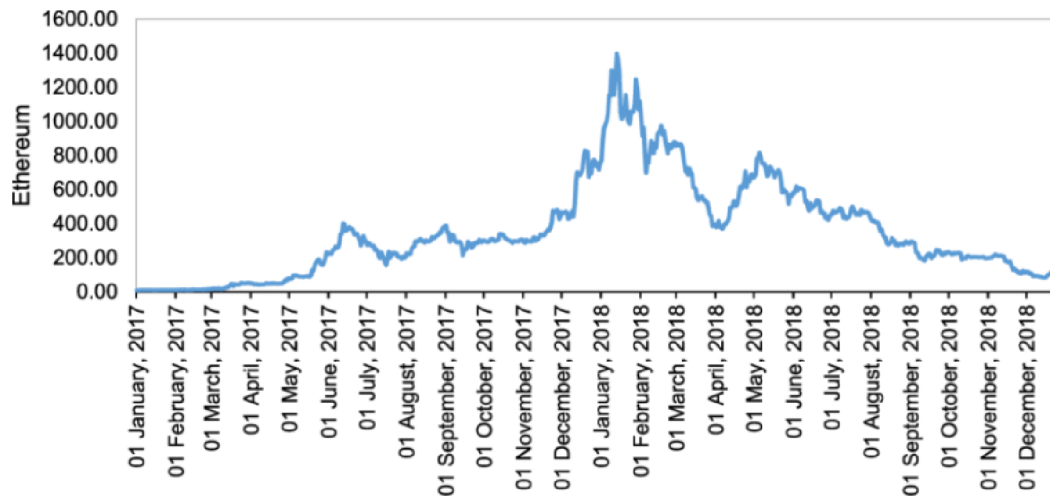


Figure 6. Ethereum's Price History by month from January 2017 until December 2018. Retrieved from https://www.researchgate.net/figure/Ethereum-Price-Line-Graph-Source-Authors-own-computations-from-data-extracted-from_fig2_350837295

Reasons for the Popularity of Cryptocurrencies on the Dark Web

The DarkNet is an encrypted network, access to the personal data of users of which cannot be obtained just like that. Digital coins, such as Bitcoin and the like, provide absolute or partial (but also quite high) anonymity in transactions.

In this regard, the Dark side of the Internet, as the Darknet is sometimes called, has become heavily dependent on cryptocurrencies. Anonymous transactions with tokens allowed the network to develop by leaps and bounds, so many people who do not understand the essence of digital coins consider Bitcoin and altcoins to be something illegal.

Prospects for the DarkNet and Cryptocurrencies

According to experts from the Chainalysis portal, distributed crime can flourish in 2022-2023. Criminal activity is moving to distributed platforms, which creates the strongest challenge for intelligence agencies and law enforcement agencies.

Analysts believe that criminal gangs and organizations will leave the DarkNet network, moving to encrypted applications like Telegram, WhatsApp or Signal. Some platforms already today have channels for people who engage in illegal activities.

Increasingly, cryptocurrencies appear in the underworld, and this trend is only growing every month. Many criminal groups are already actively using Bitcoins and altcoins today, using the services of experts in the cryptocurrency world. The latter provide criminals with recommendations on the introduction of digital assets into fraudulent schemes, help launder money and engage in illegal gambling. There are already real cases when cartels took control of miners and entire exchanges in order to launder money through them.

Another challenge to cryptocurrencies can be made to law enforcement agencies if they are used by individuals and entire states to circumvent international sanctions. All this in the future can create a real threat to cybersecurity.

5. Analysis and Conclusion

In the previous parts of this paper, it has been established that cryptocurrencies are highly regarded for their anonymity (although not complete) and are used as one of the main methods of payment for uncontrolled transactions (including illegal transactions).

If the transactions in the Dark web had to be carried out using standard banking accounts, then special services would have had no trouble arresting both sides of transaction. However, with the introduction of Bitcoin and altcoins, users of the Dark web got a means of almost complete impunity to conduct illegal activities. In return, the rates and demand on cryptocurrencies have skyrocketed. For example, when Bitcoin was originally created in 2008, it had a price of virtually \$0 per Bitcoin. As of today, one Bitcoin is worth more than 28 thousand dollars.

Moreover, 4 examples of the Dark web marketplaces have been studied:

- The Silk Road is one of the first marketplaces to accept cryptocurrency as a method of payment.
- The estimated turnover of DarkMarket was 4,650 Bitcoins and 12,800 – which was approximately €140 million at that time.
- Both AlphaBay and Oasis added Monero and Ethereum as payment methods, which caused these cryptocurrencies' rates to increase almost 4 times.

And these examples are just a tip of the iceberg – while some markets get shutdown, others take their place. But it is quite clear that there is a connection between cryptocurrencies and the Dark web – cryptocurrencies are pretty much the only safe method of payment for the users of the “Dark side of the Internet”.

To conclude this research, it would not be an exaggeration to say that the intelligence services of the leading countries of the world are closely watching the developing cryptocurrency market. As a result, even with the observance of all methods of conspiracy, it is most often not possible to hide transfers of huge amounts in cryptocurrency. Suspicious transactions can cause close interest of special services in one or another person. As a result, the issue of privacy and its significance for each person has reached a new, previously inaccessible level.

Key words: *currency, cryptocurrency, the Internet, the Dark web, anonymity, illegal*

Bibliography

Printed sources

- Antonopoulos, A. M. (2014). *Mastering Bitcoin: Programming the Open Blockchain*.
- Dawkins, R. (2016). *The Selfish Gene*.
- Eddison, L. (2018). *Tor and The Deep Web: The Complete Guide to Stay Anonymous in The Dark Net: Two Manuscripts In one*.
- Extance, A. (2015). *The future of cryptocurrencies: Bitcoin and beyond*.
- Fisher, M. (2010). *Capitalist Realism: Is There No Alternative?*
- Green, C. & Farland, D. & Read, D. T. (2018). *Silk Road Takedown*.
- Hausman, D. (2012). *The Philosophy of Economics*.
- Kosseff, J. (2019). *The Twenty-Six Words That Created the Internet*. Cornell University Press.
- Liotard, J. F. (1998). *The Postmodern Condition*.
- Mainelli, M., & Smith, M. (2015). *Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)*.
- Mankiw, N.G. (2004). *Essentials of Economics*. Third Edition.
- Ozkaya, E. & Islam, R. (2019). *Inside the Dark Web*.
- Paganini, P. & Amores, R. G. (2012). *The Deep Dark Web: The Hidden World*.
- Popper, N. (2015). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*.
- Rodgers, E. J. (2018). *What is the Dark Web? The Truth about the Hidden Part of the Internet*.
- Ryan, J. (2013). *A History of the Internet and the Digital Future*. Reaktion Books.
- Swan, M. (2015). *Blockchain: Blueprint for a New Economy*.
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world*.

Von Weizsäcker, E., & Wijkman, A. (2018). *Come on! Capitalism, Short-termism, Population and the Destruction of the Planet*.

Williams, J. (1997). *Money. A History*. British Museum Press.

Electronic sources

Ashford, K. & Schmidt, J. (2022). What Is Cryptocurrency? *Forbes*. Retrieved from <https://www.forbes.com/advisor/>

Bernstein, E. & Sommers, C. (2020). Inside the FBI takedown of the mastermind behind website offering drugs, guns and murders for hire. *CBS News*. Retrieved from <https://www.cbsnews.com/>

Bloomenthal, A. (2021). Dark Web. *Investopedia*. Retrieved from <https://www.investopedia.com/>

Bloomenthal, A. (2022). What is the Dark Web and Should you Access It? *Investopedia*. Retrieved from <https://www.investopedia.com/>

Capital.com Research Team. (2019). Types of Cryptocurrencies: Explaining the Major Types of Cryptos. *Capital*. Retrieved from <https://capital.com/>

Domm, P. (2017). Bitcoin is already dwarfing some of the largest financial market bubbles of all time. *CNBC*. Retrieved from <https://www.cnbc.com/world/>

Europol. (2021). 150 arrested in Dark web drug bust as police seize €26 million. *Europol*. Retrieved from <https://www.europol.europa.eu/>

Frankenfield, J. (2022). Currency: What It Is, How It Works, and How It Relates to Money. *Investopedia*. Retrieved from <https://www.investopedia.com/>

Hern, A. (2014). Cicada 3301: I tried the hardest puzzle on the Internet and failed spectacularly. *The Guardian*. Retrieved from <https://www.theguardian.com/international>

Kastner, E. (2020). History of the Dark web [Timeline]. *SOS can help*. Retrieved from <https://www.soscanhelp.com/>

Knight, R. (2022). Ross Ulbricht: The Real Story Behind the Silk Road Founder. *Be in Crypto*. Retrieved from <https://beincrypto.com/>

Main Types of Cryptocurrencies. Coins and Tokens. (n.d.). Retrieved from

<https://easycryptostart.com/>

McCormick, T. (2013). The Darknet: A Short History. *Foreign Policy*. Retrieved from

<https://foreignpolicy.com/>

Metais, J. (2020). Silk Road. *Coin Desk*. Retrieved from <https://www.coindesk.com/>

Sparkes, M. (n.d.). What is Bitcoin and how does it work? *New Scientist*. Retrieved from

<https://www.newscientist.com/>

Tamplin, T. (2023). What is Ethereum? *Finance Strategists*. Retrieved from

<https://www.financestrategists.com/>

Ullman, M. (2022). How Inflation Affects Your Cost of Living. *Investopedia*. Retrieved

from <https://www.investopedia.com/>

List of pictures

Figure 1. *Bitcoin's Price History*. Retrieved from

<https://coinmarketcap.com/currencies/bitcoin/>

Figure 2. *Cicada 3301's first puzzle*. Retrieved from

<https://www.wnycstudios.org/podcasts/notetoself/articles/meet-teenage-codebreaker-who-helped-solve-cicada-3301-internet-puzzle>

Figure 3. *A poster found in Warsaw shows a QR Code for a website related to the Cicada*

3301 mystery. Retrieved from <https://www.npr.org/2014/01/05/259959632/the-internets-cicada-a-mystery-without-an-answer?t=1643081756420>

Figure 4. *Ross William Ulbrich. The creator of the Darknet market website "the Silk*

Road". Retrieved from <https://www.wsj.com/articles/silk-road-trial-ross-ulbrichts-fate-sits-with-jurors-1423007681>

Figure 5. *Monero's Price History*. Retrieved from

<https://coinmarketcap.com/currencies/monero/>

Figure 6. *Ethereum's Price History by month from January 2017 until December 2018*.

Retrieved from https://www.researchgate.net/figure/Ethereum-Price-Line-Graph-Source-Authors-own-computations-from-data-extracted-from_fig2_350837295