CRYPTOCURRENCY OPERATING PRINCIPLE, MARKET AND RISKS

Pataki Péter Gergely – Zörög Zoltán

Abstract

Over the last decade or 1 - 1.5 years, financial markets have witnessed the mass emergence of virtual currencies based on blockchain technology, also known as cryptocurrencies. The most widely known is Bitcoin, the first representative, but today there are around 22,500 other cryptocurrencies. Many people see cryptocurrencies as an investment product with a high potential return, but are not aware of their operating mechanisms and the risks involved. There is a lively debate in financial circles on whether and to what extent crypto-currencies and their markets should be regulated. This paper will provide an overview of the characteristics of cryptocurrencies, their main types, possible directions for further development and the risks they entail, based mainly on international literature.

Keywords: *cryptodeviza, Bitcoin, Altcoin, CBCD, risks*
JEL: *O16, O33*

Introduction

The mechanism of crypto currencies is not as simple and easy to understand as the average person might think. Many people believe that Bitcoin was the first cryptocurrency, and they are partly right, but the idea of creating a virtual currency had been around for some time. Cryptocurrencies are generally defined as currencies that are designed to function both as money and as a means of payment and are not controlled by a person, group or organisation, so there is no need for a third party to be involved in financial transactions. Blockchain miners are rewarded for their work in verifying transactions with a particular cryptocurrency, which can be traded on multiple exchanges. But how exactly did the crypto market emerge?

Material and method

This paper presents a synthesis of the available literature on crypto-devices, organised by topic. Due to the very limited databases available, it is not possible to carry out statistical-mathematical analyses on the subject under study.

Results

Historical overview of the development of crypto-devices

In 1983, an American cryptographer named David Chaum invented a type of cryptographic electronic money called ecash. It was implemented through a company called Digicash and used as a

micro-payment system by 2 US banks between 1995 and 1998. Digicash required user software to extract the banknotes from the bank and assign specific encryption keys before they could be sent to the recipients. This allowed the digital currency to be untraceable by third parties. (Chaum et al. 1990)

In 1996, the National Security Agency published a document entitled: How to Make a Mint: The Cryptography of Anonymous Electronic Cash. A cryptosystem is described in this document. The study was published in The American Law Review in 1997, but before that it had already appeared on the MIT mailing list in the same year. (Law et al. 1996)

In 1988, Wei Dai created "B money", which was a distributed electronic money system. Soon after, Nick Szabo described the so-called Bit Gold. (Wei 1998) Bit Gold has never been implemented, but has been called "a direct precursor to the Bitcoin architecture". In Szabo's Bit Gold structure, a participant's computing power is devoted to solving cryptographic puzzles. In a Bit Gold network, solved puzzles would be posted to the Byzantine Bug Public Registry and assigned to the solver's public key. Each solution would become part of the next challenge, creating a growing chain of new features. This aspect of the system gave the network the opportunity to check and timestamp the new coins, because if the majority of the parties did not agree to accept the new solutions, they could not start the next puzzle. However, it should be noted that if we try to plan transactions with digital coins, we run into the "double spending problem". Once data has been created, reproducing it is a simple copy and paste operation. Most digital currencies solve this problem by handing over part of the control to a central authority that keeps track of the balance of each account. This was an unacceptable solution for Szabo. "I have tried to emulate as much as possible the security and trust characteristics of gold in cyberspace, the most important of which is that it is not dependent on a trusted central authority," - he said. (Szabo 1998)

Bitcoin was created in January 2009 by a developer named Satoshi Nakamoto. He used the SHA-256 cryptographic hash function in his proof-of-work system. (Satoshi 2009) This was followed in April 2011 by the creation of Namecoins, an attempt to create decentralised DNA. In October 2011, Litecoin was launched, which used scrypt instead of SHA-256 as the hash function. Peercoin was created in August 2012 using a hybrid of proof-of-work and proof-of-stake. (https://www.namecoin.org/)

On 6 August 2014, the UK announced that the Treasury had carried out a study into cryptocurrencies and what role, if any, they could play in the UK economy. The study also addressed the question of whether regulation should be considered. In 2018, a study was published in which it was described that cryptocurrencies pose new challenges to the current regulatory framework and that the complexity of certain types of cryptocurrencies makes it difficult to determine which regulatory scope they fall under.

The combined market capitalisation of all cryptocurrencies has been calculated since 2013. In 2017, they reached the $100 billion aggregate market capitalisation for the first time, rising to a temporary peak of $800 billion in January 2018. It then fell below $500 billion within a few weeks. This limit was not exceeded again until November 2020. Prices then literally exploded, reaching a preliminary peak on May 12, 2021, when total market capitalization exceeded $2.5 trillion. Cryptocurrencies, with the exception of so-called stablecoins, fall into the highly volatile category. The trading price of all cryptocurrencies is also directly linked to the valuation of Bitcoin and, generally speaking, it decreases when the price of Bitcoin falls and vice versa. All coins and tokens that are not Bitcoin are grouped under the term altcoins (hence alternative coins). (Ciaian et al. 2018)

Table 1. The ten most capitalised cryptocurrencies on 22.02.2023

Cryptocurrency		*Appearance*	*Exchange rate*	*Capital value*
Bitcoin	BTC	2009	$24036.54	$463.607.383.344
Ethereum	ETH	2015	$1635.06	$200.208.225.757
Tether	USDT	2014	$1.00	$70.469.157.065
BNB	BNB	2017	$307.93	$48.664.608.488
USD Coin	USDC	2018	$0.9999	$42.228.703.663
XRP	XRP	2012	$0.3925	$20.009.606.119
Cardano	ADA	2017	$0.3854	$13.354.257.701
Binance USD	BUSD	2019	$1.00	$12.435.806.702
Polygon	MATIC	2020	$1.36	$11.890.013.478
Dogecoin	DOGE	2013	$0.08532	$11.324.744.013

Source: own editing, coinmarketcap.com, 2022

According to Jan Lansky (2018), cryptocurrency is a system that meets six conditions:

- The system does not need a central authority; it is maintained by a distributed consensus.
- The system tracks crypto currency units and their ownership.
- The system determines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the conditions for their creation and how ownership of the new units can be determined.
- The ownership of cryptocurrency units can only be proven cryptographically.
- The system allows transactions that change the ownership of cryptocurrency units. Transaction instructions can only be issued by an entity that confirms the current ownership of these units.
- If two different instructions to redeem ownership of the same cryptographic units are given at the same time, the system will execute at most one of them.

The way crypto currencies work

A currency without intrinsic value can only work if there is a sufficient degree of trust between the participants. In the case of conventional fiat money, the central bank must be trusted, or the central bank or the state imposes the use of money through coercion, monopoly of power and state power, regardless of the trust or distrust of the public. In the case of cryptocurrencies, new issues and transactions are confirmed by the majority of participants, who are essentially distrustful and in control of each other.

Verification process

As binary information can be reproduced almost at will, it must be ensured - as with any other cashless payment system - that the amount in circulation does not grow uncontrollably. Thus, a transaction is only valid if the sum of the inputs (accounts from which a certain amount is deducted) equals the sum of the outputs (accounts to which a certain amount is added). The only exception

is new issues, which also have to follow pre-defined rules that everyone can understand in order to achieve the necessary confidence. (Tyson 2022)

For standard cashless payment transactions, the participant must rely on an operating entity (bank, credit card company or similar) to monitor and enforce compliance. In the case of crypto currencies, this is the responsibility of the community of all participants. Corrections to the system are only possible if a majority of participants agree to them by request. In the case of Bitcoin, for example, on 15 August 2010, due to a software bug, the majority automatically accepted a transaction that did not comply with the rules. This transaction resulted in 184 billion BTC (bitcoin) being credited to two accounts. This has led to a sudden multiplication of the money supply and thus to a drastic inflation of existing credit. This error could have been corrected by releasing new, improved software that rejects these transactions because they did not comply with the rules. However, since no one could fix the distributed database of all transactions, the bug was only fixed when the majority of participants had used the new software long enough to build a new, longer and thus higher priority blockchain by confirming transactions. (Stevens 2020)

Transaction fees

Not least to avoid overload attacks (denial of service attacks) against the operation of cryptocurrency, crypto exchanges impose transaction fees to avoid pointless transfers of very small amounts. These transaction fees are calculated by the new block creator transferring the agreed amount to their own account. Transaction fees thus provide an incentive to participate in the creation of new blocks, in addition to new emissions. Thus, they provide an economic incentive to participate even if there are no (more) new issues to come.

Because block sizes are limited, transactions have to wait longer to be moved to a new block. If the originator of the transaction wants to speed up this process, he can voluntarily include an increased transaction fee in his transfer order. Other participants prefer to add this transaction to their new blocks in order to book the increased transaction fee for themselves.

The mining of cryptocurrencies

Using as much computing power as possible to have a better chance of profiting from new releases is also called mining. As cryptocurrencies are traded for real assets and are also exchanged for conventional currencies, there is a real economic incentive to solve the specific mining-related solving tasks as efficiently as possible. This led to the use of increasingly specialised hardware. Initially, standard processors used in PCs were used, soon followed by implementations using graphics processors. Meanwhile, devices based on field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs) are being developed specifically for this purpose. This has led to a huge increase in computing power. For Bitcoin, for example, the computing power used increased 660-fold between January 2013 and January 2014. For an individual user with an average PC, it has become almost impossible to participate in new issues or crypto currencies that attract transaction fees, where there is competition for computing power.

To cope with this effect, the increasing number of participants and Moore's Law, the difficulty level of the computational tasks for cryptocurrencies can be adjusted. Thus, participants will only accept solved tasks that meet a predefined and regularly set difficulty level. In this way, emission rates can be kept constant and the effort needed for any manipulation can be increased. The proof-of-work and share ownership principles can be combined. Thus, owners of large, preferably old

balances can submit solutions with reduced difficulty to Peercoin. The resulting increased chance of receiving new issues or transaction fees is seen by the creators of krip money as a form of interest of these credits. (Stevens 2020)

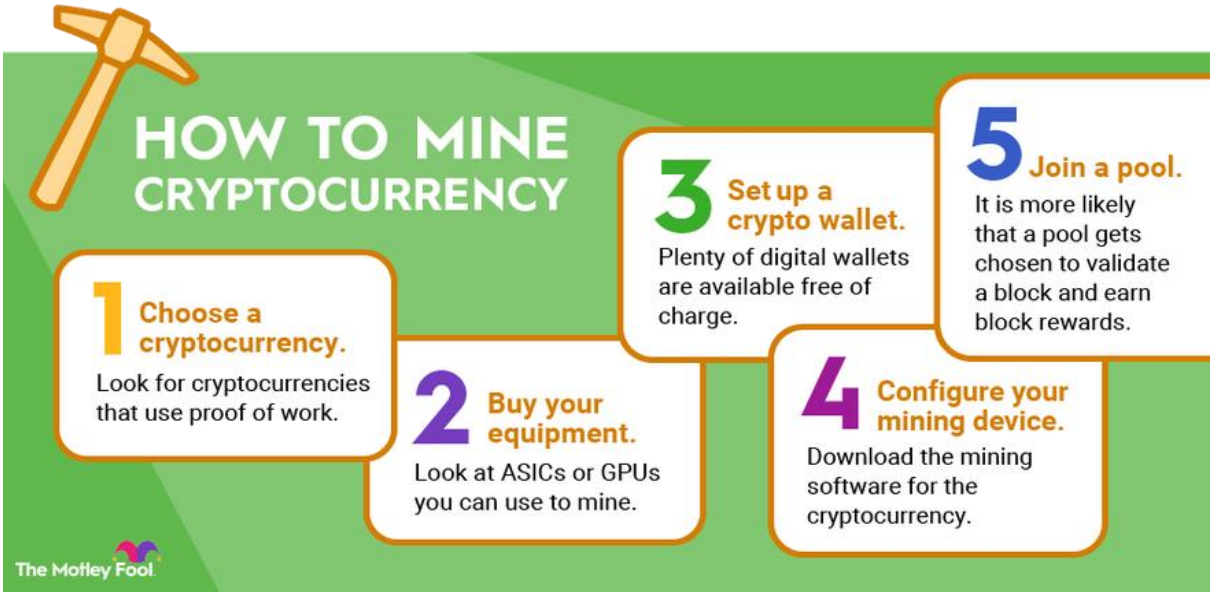

Figure 1. : The initial steps of crypto currency mining

Source: https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/how-to-mine/

P2P networking of participants and Accounting process

There are hundreds of specifications for implementing crypto currencies. Some of them operate on similar principles to Bitcoin and are similar in structure. (Satoshi 2009)

All participants communicate with each other through a peer-to-peer network. Every message that a participant sends to this network becomes available to everyone else. However, they are not sent as a broadcast, but as is usual in P2P networks, they are sent one by one. A message sent to this network is therefore equivalent to a public message to all participants. (Ali et al. 2015)

So far, cryptodeviza consists only of a P2P network where messages signed with asymmetric cryptography are published. The essential part is therefore a special form of accounting. It consists of data blocks, each of which refers to its predecessor, forming a chain, the blockchain. Each data block is a new page in the common accounting. Each participant who wishes to add a new block to this ledger can add a transaction from scratch to his/her own account, in addition to the newly accumulated transactions to be confirmed. You will then receive the new issue's tranche linked to this block, as required by the rules. Many participants are therefore happy to create and publish such new blocks.

The difficulty of creating new blocks to limit new issues. To do this, a one-way function implemented as a cryptological hash function must be computed from the block. This hash value must meet a generally recognised criterion to be recognised as a valid new block. In the simplest case, the value should be below a certain limit. The lower this threshold, the lower the probability that the newly calculated hash value will be below it. Accordingly, it is more difficult to create such a block. The participant must modify the block until it creates a valid block with a hash value below the limit. To this end, each block contains a value called nonce, whose only function is to change

until the hash value of the entire block satisfies the condition. Since this is a one-way function, it is not possible to directly calculate the required nonce. The difficulty is therefore that the hash value of the modified blocks has to be calculated until it accidentally falls below the specified threshold. The hash functions used by different crypto currencies include SHA-2 (Bitcoin, Pe-ercoin), SHA-3 (Copperlark, Maxcoin), Scrypt (Litecoin, Worldcoin) and POW (Protoshares). (Larimer 2014).

Cryptocurrencies and other types of settlement units similar to cryptocurrencies

The Bitcoin

Bitcoin is the first and best-known cryptocurrency on the market worldwide, based on a decentralised booking system. Payments are cryptographically authenticated (digital signature) and are made over a peer-to-peer network of peer computers. Unlike traditional banking, a Bitcoin transaction is equivalent to a settlement between the parties involved. Bitcoin ownership is stored in personal digital wallets (colloquially "wallets"). The Bitcoin price follows the principle of stock exchange pricing compared to legal tender (fiat money). (Kannenberg 2014)

The Bitcoin payment system was developed by a person or group under the pseudonym Satoshi Nakamoto in 2007, described by Satoshi (2008) in a self-proclaimed publication in November 2008 - the so-called white paper - and published in January 2009 together with open source reference software. The Bitcoin network is based on a decentralised database, a blockchain shared by all participants, in which every transaction ever made is verifiably recorded. Cryptographic techniques ensure that Bitcoin can only be used for valid transactions by its owner, without exception, and that the same units of currency cannot be spent more than once. (Chohan,2022)

Bitcoin can be considered both a payment system and a monetary unit that is managed or created decentrally on a computer network using proprietary software. The only condition for participation is the use of a Bitcoin client or an online service that provides this functionality. As a result, the Bitcoin system is not subject to geographical restrictions - except for the availability of an internet connection - and can be used across borders.. (Kannenberg 2014)

The Bitcoin payment system therefore consists of a database, the blockchain, a kind of logbook in which all Bitcoin transactions are recorded. The Bitcoin payment system uses a peer-to-peer network to which all participating computers connect via a program. All Bitcoin transactions are recorded in this Bitcoin network. The blockchain is redundantly and decentrally stored on each Bitcoin node, managed and continuously updated via the Bitcoin network.

The Altcoins

Apart from Bitcoin, all cryptocurrencies are known collectively as altcoins. The second largest cryptocurrency has been called Ether for years and is the internal currency of the Ethereum blockchain system. The majority of the more than 20 000 cryptocurrencies that exist today were not born as pure payment systems. Instead, the majority of cryptocurrencies, known as coins or tokens, are indeed exchangeable and tradable assets, according to the six terms of the definition previously mentioned by Lansky (2018), but with additional features compared to mere currency. These additional added values or features vary greatly. For example, there are crypto currencies that provide voting rights for various decisions within the network (or external factors), crypto

currencies that represent a current value equivalent to fiat currencies, crypto currencies that are used solely as a transaction fee for a network, or crypto currencies that allow a warehouse to communicate with the appropriate supplier, and many other possibilities arise.

Apart from Bitcoin, all cryptocurrencies are known collectively as altcoins. The second largest cryptocurrency has been called Ether for years and is the internal currency of the Ethereum blockchain system. (https://ethereum.org/en/eth/)

Central Bank Digital Currency

The term central bank digital currency (CBDC) refers to projects that involve a digital currency issued by a public central bank. The value of the CBDC must be equal to the value of the represented traditional (national) currency in a 1:1 ratio.

The Bank for International Settlements report states that although the term "digital central bank currency" is not precisely defined, it is "considered by most to be a new form of central bank money [...] distinct from traditional reserve or clearing account balances.". (Morten et al. 2017)

CBDCs also differ from virtual currencies and cryptocurrencies in that the latter are not issued by a state and do not have the legal tender status declared by the government.

Generally speaking, CBDCs are at a very early stage of development. According to a survey in 2021, around 80% of central banks worldwide are considering CBDCs and 40% have already tested the concept. (Codruta et al. 2021)

Privacy Coins

Privacy coins are crypto currencies that allow digital anonymous payments (digital cash). When Bitcoin was first introduced, it was still considered a privacy coin, and was used as a means of payment in many "darknet" marketplaces. However, due to the increasing integration of cryptocurrencies into existing government payment systems, regulatory requirements such as KYC (know your customer) or anti-money laundering laws have led to a softening of anonymity in the Bitcoin ecosystem. Bitcoin transactions are therefore not anonymous, but merely pseudonymous. Attempts are therefore being made to extend the anonymity that exists in the Bitcoin ecosystem to the fullest possible anonymity. The beginnings of privacy coins and digital cash can be found in the cryptoanarchy and the cypherpunks' network. (May 1988)

Privacy coins therefore represent a subset of cryptocurrencies that make it difficult to trace the ownership of coins and restore the substitutability of a payment instrument similar to the former banknotes. With the growing popularity of digital currencies and the European Central Bank's (ECB) plans to introduce a digital euro, consumers are increasingly demanding greater privacy protection. In a survey of citizens, associations and experts on the digital euro conducted by the ECB between November 2020 and January 2021, 43% of the 8,200 respondents cited privacy as the most important issue. (ECB 2021)

Figure 2. : Types of privacy coins
Sources: https://comparebrokers.co/compare/privacy-coins/

The emergence of institutional investors in the cryptocurrency market

In 2021 and 2022, cryptocurrencies underwent an unprecedented institutional adjustment, especially Bitcoin, which also boosted the prices of virtually all cryptocurrencies. Square, MicroStrategy and Tesla are just three of the many companies already investing in Bitcoin.

In June 2021, Grayscale Bitcoin Trust had $25.7 billion under management. According to a June 2021 survey of 100 hedge fund financial managers worldwide by fund manager Intertrust, these managers expect to hold an average of 7.2 percent of their assets in cryptocurrencies within five years. Intertrust estimates that, if this spreads to the industry as a whole, the hedge fund industry as a whole could have around $312 billion in assets invested in cryptocurrency. (Fletcher 2021)

In Canada, three Ethereum ETFs were approved on 20 April 2021, following the approval of a Bitcoin ETF in February 2021.Both Bitcoin and Ethereum ETFs were approved in 2022. 2022 ProFunds, a global asset manager with $60 billion under management, successfully registered a Bitcoin futures mutual fund with the US Securities and Exchange Commission (SEC) on 27 July. (Campbell 2021)

The listing of Coinbase, one of the largest and longest-established companies in the still young industry, is also expected to make a big splash in April 2021. The IPO was the largest since Facebook's in 2012 and the first company whose business model is based solely on trading and betting on cryptocurrencies.

Criticisms and risks of cryptocurrencies

Software error

Crypto currencies, like all software-driven systems, are not free from software bugs.
Examples:

- The transfer of 184 billion BTC (never more than 21 million BTC) on 15 August 2010 was based on an arithmetic overflow. (Stevens 2020)
- On 11 March 2013, the Bitcoin blockchain split into two branches, considered valid by different groups of participants. For this reason the ledger was inconsistent. The cause was an accidental incompatibility of a new software version. This generated blocks that were rejected by older versions because they did not comply with the rules. The case also proves that mining pool operators or powerful hardware have a special influence on crypto currencies. System operators are asked to restore their systems at short notice until a patched version is available.
- In June 2022, California-based Harmony lost $100 million worth of crypto in an attack on its software.

So far, in the case of bitcoin, all the confusion has been resolved by patching the software and the cooperative behaviour of the parties involved. However, there is no guarantee that this will be the case for all cryptocurrencies at all times. In light of this, the statement at the beginning that there is no single point of failure must also be put into perspective. If a cryptocurrency runs almost exclusively on software derived from a single source code, and there are no independent implementations, this source code represents a single point of failure.

Right of disposal

As the control of credit balances in cryptocurrency is only available through secret private keys, credit balances have been irretrievably lost in the past due to data loss. Reimbursement by other means is generally impossible, as lost credit is in principle indistinguishable from used and currently unused assets. This also means that only the maximum, but not the actual amount of money that can be traded is known. (Orsini 2014)

Private keys to control credit are therefore a target for cybercriminals. 400 000 completed cases of cryptocurrency fraud are estimated by 2020 and further increases are predicted. Given the worldwide operation under pseudonyms, the prosecution of such theft of cryptoassets is unlikely to be promising. As a result, companies now offer the custody of cryptoassets as a service. (Trentmann 2014)

Incorrect legal classification

In some countries, it is not clear whether cryptocurrencies are assets at all or not. This has consequences for inheritance law, for example: in Switzerland, cryptocurrencies are not considered as tangible assets, cash, receivables or securities.. Crypto assets are unlikely to be inventoried in the absence of written evidence and a counterparty (e.g. a bank). However, if an heir knows the wallet password and transfers the deceased's crypto assets to himself, it is disputed among legal experts

whether the act constitutes embezzlement and whether other heirs can take action against it. Likewise, the transfer of crypto-currencies can circumvent the provisions on advance inheritance payments and compulsory portions.

The classification of crypto-evidence as a thing is defeated by the numerus clausus of the law of things: all legal forms of things are definitively prescribed by law, but the crypto-token would correspond to a new kind of thing. In contract law, any legal form could be chosen - for example, a digital, cryptographically signed bill of exchange could be issued as a means of payment. However, all instruments covered by the law of obligations require a clearly identified counterparty, the issuer. This is not a prerequisite for the widespread use of cryptocurrencies. So legal clarity only applies if someone holds a crypto-based security, such as a certificate or a share of a fund, instead of a crypto currency. (Lukas et. al 2021)

Distribution, Exchange rate fluctuations and price manipulation

Some crypto currencies are designed so that a significant proportion of new issuance has already been pre-mined by the founders. They often contain rules that provide particularly favourable conditions for those in the start-up phase, the so-called early adopters. When founders are accused of self-serving intent, such cryptocurrencies are also known as scam coins. However, pre-mining can also be an openly documented part of the concept. (Morris 2013)

Crypto currencies are risky due to their high volatility and are potential targets for pump-and-dump attacks. Pump and dump attacks are a form of securities fraud, whereby false and misleading positive statements are used to artificially inflate the price of shares held in order to sell shares bought cheaply at a higher price. The well-known software developer John McAfee was imprisoned in Spain until his death on charges including. Elon Musk, who in 2021 posted a series of tweets that directly addressed Bitcoin and Dogecoin cryptocurrencies, faces the same accusations. The tweets on Dogecoin were all positive, pushing the coin's price to unimaginable heights, while Musk's tweets on Bitcoin were both positive and negative, earning him numerous pump-and-dump accusations. Whether intentionally or not, the price of Bitcoin has fluctuated by at least a few percent for every Musk Bitcoin tweet in 2021, which has always had a direct impact on almost all other existing cryptos, which tend to fall when the price of Bitcoin falls, and vice versa. In 2021, Musk was also issued a warning by Anonymous for his treatment of his power over markets.

Ransom receivables

Internationally, ransomware attacks based on crypto currencies have become "more common" since the beginning of 2019. On 9 January 2019, for the first time in Norway, such a currency - the Monero. Companies and public institutions are also sometimes faced with ransom demands in cryptocurrencies as a result of ransomware attacks. Most recently, the May 2021 cyber-attack on Colonial Pipeline, which led to gasoline shortages in parts of the US, attracted attention. After paying 75 Bitcoin, the previously blocked pipeline was unblocked. The FBI was able to recover 63.7 percent of the seized Bitcoin a few weeks later, but media reports that the FBI had "hacked" the Bitcoins proved to be unfounded. (Phan 2021)

Scam

As crypto currencies are not yet state-controlled and can be issued by anyone, quite a lot of coins are offered by criminals. One such coin was the "SQUID" coin, named after the popular TV series Squid Game. Various major news outlets, such as CNBC and the BBC, reported very large, positive price jumps for the SQUID - following which the coin's online presence was cancelled and its value plummeted from $2,856 to almost zero. It was designed so that SQUID could only be bought, but it was virtually impossible to sell. The makers of SQUID made a profit of around $3.38 million. (Novak 2021)

The phenomenon of service providers collecting investors' money and then running away is known in the industry as "rug pulling". One company estimates that by 2021, USD 7.7 billion will have been raised worldwide through such "rug pulls". These included the case of Thodex in Turkey, whose founder disappeared with $2 billion. (Claburn 2021)

Money laundering and tax evasion

The quasi-anonymous (i.e. pseudonymous) nature of crypto currencies and the existence of the aforementioned mixed services make crypto currencies presumably very attractive to money launderers, as the monitoring of money laundering activities in this area is still in its infancy. However, it is possible to use artificial intelligence to monitor suspicious transactions in real time, as HSBC bank does, but this may fail because a criminal user will only use their wallet for a short period of time, for a one-off transaction. On the other hand, there is the idea that companies operating in the crypto sector should only accept clearly identified customers. (Faccia et al. 2020)

Due to the anonymous nature of cryptocurrencies and the fact that the owners of the coins are not known - while the issuers of bank accounts and securities are known to the authorities - it is virtually impossible for tax authorities to verify taxpayers' cryptocurrency assets. An important exception to this is if the wallet ID is already known to the authorities, for example through a previous payment relationship. Also, anyone can create as many wallets as they want to disguise their wealth. However, tax authorities ask taxpayers to declare their crypto assets under "other assets". However, there are crypto miners and investors who deliberately use cryptocurrencies as a means of tax evasion. (Marian 2014)

Conclusions and proposals

Based on a synthesis of foreign literature, it can be concluded that the conceptual interpretation of crypto-devices and their definition in terms of content is not uniform. In addition, in recent years, clearing units have emerged that can also be categorised as cryptocurrencies, but their operating mechanism is not exactly the same as that of classic cryptocurrencies. In recent years, previous experience has confirmed that cryptocurrency prices are highly volatile and the collapse of the FTX exchange in 2022 proved that the market framework also has serious shortcomings. However, in addition to the increasingly widespread exchange rate risk, cryptocurrencies also carry other risks and offer the potential for serious abuses. Technical solutions to mitigate exchange rate risks already exist (e.g. stablecoins as altcoins), but the lack of a single central regulation means that other risks cannot be managed. The need for a single central regulation is becoming more and more

acute, but the extent and the way to implement it is still a matter of debate among financial professionals. We believe that cryptocurrencies will continue to expand the range of financial instruments in the coming years and decades. In order to prevent the use of these financial products from causing personal tragedies due to the financial losses suffered, widespread education is needed to ensure that those concerned are able to understand and recognise the specific features of how these financial products work and the risks they entail. In the medium term, we see the need for uniform central regulation at international level.

References

[1.] Abad-Segura E. – Infante-Moro A. – González-Zamar M.-D. – López-Meneses E. *(2021):* Blockchain Technology for Secure Accounting Management: Research Trends Analysis. *Mathematics,* 9(14), 1631. https://doi.org/10.3390/math9141631

[2.] Faccia A. – Moşteanu R. N. – Pio L. – Cavaliere L. – Jose Mataruna-Dos-Santos L. *(2020):Electronic Money Laundering, The Dark Side of Fintech: An Overview of the Most Recent Cases, ICIME 2020: Proceedings of the* 2020 12th International Conference on Information Management and Engineering, pp 29–34. https://doi.org/10.1145/3430279.3430284

[3.] Kannenberg A. (2014): Kryptogeld-Regulierung in Deutschland: "Bitcoins fair behandeln". Download date: 25/2/2023 Source:https://www.heise.de/newsticker/meldung/Bitcoin-in-der-Debatte-Kann-ich-das-meiner-Mutter-empfehlen-2427822.html

[4.] Kannenberg A. (2014): Bitcoin im Sinkflug: Schwächeanfall auf dem Weg in den Mainstream. Download date: 21/2/2023 Source:https://www.heise.de/newsticker/meldung/Bitcoin-im-Sinkflug-Schwaecheanfall-auf-dem-Weg-in-den-Mainstream-2413477.html

[5.] Boar C. – Wehrli A. (2021): Ready, steady, go? – Results of the third BIS survey on central bank digital currency, *BIS Papers, Bank for International Settlements*, number 114.

[6.] Larimer D. (2014): Momentum – A memory-hard Proof-of-work via finding birthday collisions. Download date: 12/2/2023 Source: http://www.hashcash.org/papers/momentum.pdf

[7.] Chaum D. – Fiat A. – Naor M. *(1990): Untraceable Electronic Cash, Conference on the Theory and Application of Cryptography,* pp 319–327. https://doi.org/10.1007/0-387-34799-2_25

[8.] Chaum D. (1983): *Blind Signatures for Untraceable Payments*. Advances in Cryptology*,* pp 199–203. https://doi.org/10.1007/978-1-4757-0602-4_18

[9.] Morris Z. D. (2013): Beyond bitcoin: Inside the cryptocurrency ecosystem. Download date: 16/2/2023 Source: https://fortune.com/2013/12/24/beyond-bitcoin-inside-the-cryptocurrency-ecosystem/

[10.] Taha A. – Clarke D. – McCorry P. (2015): Bitcoin: Perils of an Unregulated Global P2P Currency. Newcastle upon Tyne: Newcastle University: Computing Science, *Technical Report Series,* No. CS-TR-1470.

[11.] EZB veröffentlicht Ergebnisse des öffentlichen Konsultationsverfahrens zu einem digitalen Euro (2021). Download date: 20/2/2023 Source: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.de.html

[12.] Tschorsch F. – Scheuermann B. – Bitcoin and Beyond (2016): *A Technical Survey on Decentralized Digital Currencies, IEEE Communication Survey Tutorial,* 18, 2084–2123 https://doi.org/10.1109/COMST.2016.2535718

[13.] Valeonti F. – Bikakis A. – Terras M. – Speed C. - Hudson-Smith A. – K. Chalkias (2021): Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the

Potential of Non-Fungible Tokens (NFTs), *Applied Sciences.* 11(21):9931 https://doi.org/10.3390/app11219931

[14.] Nestler F. (2013): Deutschland erkennt Bitcoins als privates Geld an. Download date: 14/2/2023 Source: https://www.faz.net/aktuell/finanzen/devisen-rohstoffe/digitale-waehrung-deutschland-erkennt-bitcoins-als-privates-geld-an-12535059.html

[15.] Namecoin. https://www.namecoin.org/ Download date: 12/2/2023

[16.] Steadman I. (2013): Wary of Bitcoin? A guide to some other cryptocurrencies https://arstechnica.com/information-technology/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies/

[17.] Lansky J.(2018)*:* Possible State Approaches to Cryptocurrencies. *Journal of Systems Integration,* 8(1), 19–31, http://dx.doi.org/10.20470/jsi.v9i1.335

[18.] Brito J. – Castillo A. (2013) - *Bitcoin: A Primer for Policymakers,* Mercatus Center at George Mason University 2013

[19.] Orsini L. (2014): What Happens To Lost Bitcoins? Download date: 23/2/2023 Source: https://readwrite.com/what-happens-to-lost-bitcoins/

[20.] Fletcher L. (2021): Hedge funds expect to hold 7 % of assets in crypto within five years. Download date: 18/2/2023 Source: https://www.ft.com/content/4f8044bf-8f0f-46b4-9fb7-6d0eba723017

[21.] Law L. – Sabett S. – Solinas J. (1996): *How to Make a Mint: The Cryptography of Anonymous Electronic Cash,* National Security Agency Office of Information Security Research and Technology Cryptology Division

[22.] https://web.archive.org/web/20140118180710/http://cryptocur.com/overview-of-all-cryptocurrencies/ Download date: 18/2/2023

[23.] https://coinmarketcap.com/ Download date: 16/2/2023

[24.] https://comparebrokers.co/compare/privacy-coins/ Download date: 10/2/2023

[25.] https://ethereum.org/en/eth/ Download date: 16/2/2023

[26.] https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/how-to-mine/ Download date: 10/2/2023

[27.] Müller L. – Ong M. (2021): *Aktuelles zum Recht der Kryptowährungen, AJP/PJA 2/2020*

[28.] Novak M. (2021): Squid Game Cryptocurrency Scammers Make Off With $2.1 Million. Download date: 8/2/2023 Source: https://gizmodo.com/squid-game-cryptocurrency-scammers-make-off-with-2-1-m-1847972824

[29.] Tyson M. (2022): Intro to crypto wallet authentication. Download date: 22/2/2023 Source: https://www.csoonline.com/article/3671972/intro-to-crypto-wallet-authentication.html

[30.] Peck E. M. (2012): Bitcoin: The Cryptoanarchists' Answer To Cash. Download date: 5/2/2023 Source: https://spectrum.ieee.org/bitcoin-the-cryptoanarchists-answer-to-cash

[31.] Bech M. – Garatt R. (2017): Central Bank Cryptocurrencies, *BIS Quarterly Review September 2017*

[32.] Szabo N. (1998): Secure Property Titles with Owner Authority. Download date: 22/2/2023 Source: https://nakamotoinstitute.org/secure-property-titles/

[33.] Trentmann N. (2014): Londoner Unternehmen bietet Tresor für Bitcoins an. Download date: 18/2/2023 Source: https://www.welt.de/finanzen/geldanlage/article123897837/Londoner-Unternehmen-bietet-Tresor-fuer-Bitcoins-an.html

[34.] Marian O. (2013): Are Cryptocurrencies Super Tax Havens?, 112 *Mich. L. Rev. First Impressions, 38*.

[35.] Ciaian P. – Rajcaniova M. – Kancs d'A.(2018): Virtual relationships: Short- and long-run evidence from BitCoin and altcoin markets, Journal of International Financial Markets, *Institutions and Money,* 52(January), 173–195. https://doi.org/10.1016/j.intfin.2017.11.001

[36.] Stevens R. (2020): The Day Someone Created 184 Billion Bitcoin. Download date: 4/2/2023 Source: https://decrypt.co/39750/184-billion-bitcoin-anonymous-creator
[37.] Nakamoto S. (2009): Bitcoin: A Peer-to-Peer Electronic Cash System. Download date: 15/2/2023 Source: https://bitcoin.org/bitcoin.pdf
[38.] Claburn T. (2021): Cryptocurrency 'rug pulls' cheated investors out of $8bn in 2021. Download date: 27/2/2023 Source: https://www.theregister.com/2021/12/16/cryptocurrency_rug_pulls/
[39.] May C. T. (1988): The Crypto Anarchist Manifesto. Download date: 10/2/2023 Source: https://nakamotoinstitute.org/crypto-anarchist-manifesto/
[40.] Campbell T. (2021): Bitcoin ETF coming 'in a year or two,' analyst says as SEC mulls applications. Download date: 11/2/2023 Source:https://www.cnbc.com/2021/04/06/bitcoin-etf-coming-in-a-year-or-two-analyst-says.html
[41.] Phan T. (2021): *Did the FBI Hack Bitcoin*? Deconstructing the Colonial Pipeline Ransom. Download date: 20/2/2023 Source: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/did-the-fbi-hack-bitcoin-deconstructing-the-colonial-pipeline-ransom
[42.] UK launches initiative to explore potential of virtual currencies (2014). Download date: 16/2/2023 Source: https://www.theuknews.com/news/224504231/uk-launches-initiative-to-explore-potential-of-virtual-currencies
[43.] Chohan W. U. (2017): Cryptocurrencies: A Brief Thematic Review, *SSRN Electronic Journal*
[44.] Dai W. (1998): B-Money. Download date: 5/2/2023 http://www.weidai.com/bmoney.txt

A tanulmány az Új Nemzeti Kíválósági Program 22-1-I támogatásával jött létre/ The study was funded by the New National Excellence Programme 22-1-I

Authors

Pataki Péter Gergely
ORCID: 0009-0009-8888-6670
Hungarian University of Agricultural and Life Sciences
Business Informatics BA
pitegeri@gmail.com

Zörög Zoltán
PhD
ORCID: 0000-0001-6659-1278
Associate Professor
Hungarian University of Agricultural and Life Sciences
Institute for Rural Development and Sustainable Economy
zorog.zoltan@uni-mate.hu