EPS Universidad Francisco de Vitoria

Fundamentals of Computer Engineering

Practical Work 1

CRYPTOCURRENCIES

2024 - 2025

Group 1

Jorge Almirall Navarro

Miguel de Vicente Luengo

Nicolás Martínez Djekic

Johan José Merida Pérez

Hugo Prieto Petrossi

Ignacio Ramos Nicolás

Table of contents

Abstract

This project examines cryptocurrencies including the following points:

1. Technologies involved such as blockchain, consensus protocols or cryptography.
2. The advantages, such as safety and low fees; and the disadvantages like illegal use and lack of regulation.
3. An evaluation of cryptocurrencies and the potential they have based on security, regulation and acceptance.
4. Their main use.
5. Ethical review of cryptocurrencies.

All the information used in the project is taken from scientific papers and documented graphs. The aim of this project is to defend the safety of crypto used for payments and investment; and to analyze the potential risks of the lack of regulations that cryptocurrencies fall under. These issues should be resolved as soon as possible since cryptocurrencies are becoming one of the main ways of making money.

1- Introduction

Over the last few years, global trends in digitalization have always been linked to a close relationship between the economy and technology. With the crisis of 2008 came along a feeling of distrust regarding the way we currently understand money. Alongside the development of information and communication technologies, a possible alternative to conventional money was conceptualized and developed. What was the initial idea behind Bitcoin has now evolved into a massive ecosystem of different decentralized blockchains, cryptocurrencies and tokens that have given birth to a humongous number of opportunities and challenges. Finally, after the 2019 pandemic a rapid development of digital payment methods took place. This led to the appearance of new and fast forms of online payment.

1.1- Motivation

The sudden emergence of cryptocurrencies has drawn the attention of many. Being a group of university students, who lack knowledge on the topic which has caused quite a lot of controversy and misinformation in the last few years, we have become intrigued. Our motivation lies in wanting to understand cryptocurrencies and the reason for all the controversy that they have caused.

1.2- Objectives

The objectives of this research on cryptocurrencies are highly linked to our motivation. Our main objective is to understand how cryptocurrencies work, which is, understanding the technologies that lie behind the concept of cryptocurrencies, increasing our notions on the world of computing in the process. Once we get to understand the fundamental technologies behind cryptocurrencies, we have the objective of comprehending the reason for all controversy, grasping in the process an overview of the opportunities and challenges that they pose, evaluating whether the claims of renowned pro-Bitcoin activists and speakers such as Michael Saylor or Peter Thiel that cryptocurrencies are going to become the new hegemonic means of payment have a point or not.

2- Cryptocurrencies

Digital technology is at its peak, a change from analog and electronic technology to digital technology. Being in the age of digital technology, it was a matter of time that a digital form of currency would be created. The study of cryptography and the conceptualization of the blockchain, combined with the economic crisis of 2008,

pushed forward the creation of this digital form of currency, making Bitcoin a turning point in the way we conceive money, representing the first example of what we now consider a relatively common form of currency: cryptocurrencies.

Many companies and financial institutions are taking advantage of the development of the cryptocurrencies and blockchain technologies. Nowadays, cryptocurrencies and blockchain-based financial systems control part of the economic transactions. It is believed that blockchain technology is about to transform drastically the way we do business, if it isn't already doing so.[1]

La revolución de las criptomonedas. (s. f.). calameo.com. https://www.calameo.com/books/0069707689065e58d753a

2.1- Detailed overview

Cryptocurrencies are decentralized digital assets whose reliability in terms of transaction security is very high, as they have a high-level encryption. It is based on software whose function is the collection and storage of money whose digital format is sealed with end-to-end encryption. Cryptocurrencies revolve around two basic concepts. On the one hand, DLT "Distributed Ledger Technology", this technology is characterized by its permissiveness when it comes to an easy access, from several points to a synchronized data. On the other hand, the blockchain, is nothing more than a secure cryptographic structure.[2]

These currencies do not exist in physical form, only virtually, using a website for their transaction. What differentiates these currencies from other types of currencies is that for their use to be viable, both the sender and the receiver must have some

[1] Schmalz, M., & Director, P. (n.d.). *Oxford Blockchain Strategy Programme*. Saïd Business School. https://www.sbs.ox.ac.uk/programmes/executive-education/online-programmes/oxford-blockchain-strategy-programme

[2] Arner, D., Auer, R., & Frost, J. (2020, November). *Stablecoins: Risks, potential and regulation*. Bank for International Settlements. https://www.bis.org/publ/work905.pdf

knowledge of this world and be involved in it, otherwise these currencies have no value. Cryptocurrencies have a very sophisticated structure behind them, but accessing them is relatively easy, being at the reach of everyone who has the means to access the Internet.

2.2- Technologies involved

To explain the technologies involved we are going to start by explaining the technologies that are present on the surface to end with the most fundamental ones. In order, we are going to explain blockchain technology, consensus mechanisms and the cryptography fundamentals behind cryptocurrencies.

In order to work, cryptocurrencies make use of blockchain technology. A blockchain consists of a database in which the transactions and other digital events executed by the participants of the chain are recorded[3]. In this sense the blockchain works like the ledger of an accountant, registering all transactions that take place between the participants. For this reason, we categorize blockchain as being a DTL (Distributed Ledger Technology). It is distributed because the verification of the different blocks of transactions, which are linked forming a chain that starts with the genesis block, is a task that is executed by a large number of participants, ensuring decentralization. This distribution in the task of verification is possible because blockchains work like P2P (Peer-to-peer) networks, which are networks in which all nodes have the same privileges and functions.

As for the consensus there are, depending on the blockchain, different consensus mechanisms. Proof of Work (PoW) and Proof of Stake (PoS) are two of the most well-known consensus mechanisms. Proof of Work bases block verification on nodes proving that they have used enough computing resources to solve a mathematical puzzle[3] while Proof of Stake grants block verification randomly, having a higher probability of being chosen as the verifier if you hold a larger quantity of the blockchain's token.

Below the level of consensus protocols, there is the foundational aspect of cryptocurrencies: cryptography. As the name suggests, cryptocurrencies are built upon cryptographic technology that encompasses mathematical algorithms that generate public-private key pairs that are the base upon which wallets, where

[3] Crosby, M., Nachiappan, Pattanayak, P., Verma, S., & Kalyanaraman, V. (2015, October 16). *Blockchain technology - UC Berkeley Sutardja Center*. Blockchain Technology Beyond Bitcoin. https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

cryptocurrencies are stored, work. These are the hash functions that verify the integrity of the blocks of transactions and elliptical curve encryption.

In addition to the fundamental components for cryptocurrencies to work, certain blockchains like Ethereum include, apart from the mentioned, some new technologies like Smart Contracts which allow the participants of the chain to create self-executing contracts that do an action automatically if a previously agreed condition is verified as true. Smart Contracts have led to the evolution of other technologies such as NFTs, which allows people to have verified property over certain digital goods leveraging Smart Contracts.

NFT in cryptocurrencies - Bing. (s. f.). Bing. https://www.bing.com/images/search?view=detailV2&ccid=LJGBlvy8&id=CBD4424D7D3D0F369F756B0CF6BAF9A19F0312C9&thid=OIP.LJGBlvy8RyReCAn1LXJ88AHaEK&mediaurl=https%3a%2f%2frobots.net%2fwp-content%2fuploads%2f2023%2f10%2fwhat-is-an-nft-crypto-1698577486.jpg&cdnurl=https%3a%2f%2fth.bing.com%2fth%2fid%2fR.2c918196fcbc47245e0809f52d727cf0%3frik%3dyRIDn6H5uvYMaw%26pid%3dImgRaw%26r%3d0&exph=675&expw=1200&q=NFT+in+cryptocurrencies&simid=608027049168763393&FORM=IRPRST&ck=1656768C0382D4AE0F9786EDD287B1D5&selectedIndex=15&itb=0%20%20%20https://www.bing.com/images/search?view=detailV2&ccid=1FqiAlQh&id=5B93BBDDF4996EF5F1ED0DEEBF6104A4C29CCBE7&thid=OIP.1FqiAlQha8mECTWZIvozFwHaDt&mediaurl=https%3a%2f%2facademy.moralis.io%2fwp-content%2fuploads%2f2021%2f01%2fcrypto_dlt.png&cdnurl=https%3a%2f%2fth

2.3- Advantages and disadvantages

Cryptocurrencies offer an innovative alternative to traditional financial systems. Like everything else, they have advantages and disadvantages and can impact society in a way that can benefit us economically or affect us negatively.

When it comes to the advantages, crypto can be defined in three simple words, secure digital currency. The main purpose of this is to make people's lives easier when handling money. First, it is decentralized and independent, meaning it

operates without central authorities like banks or governments. This gives cryptocurrencies a better and more useful financial system than the traditional one. Compared to this traditional system, crypto transactions tend to be low-cost or even free of charge for large amounts, reducing fees that generally banks charge, plus these cheap transactions can be sent or received worldwide, making them very helpful. Cryptocurrencies use blockchain technology, which offers transaction security and protects users' personal information, so the fact that it provides us with safety, fast transactions and, most importantly, low costs is a huge problem solver.

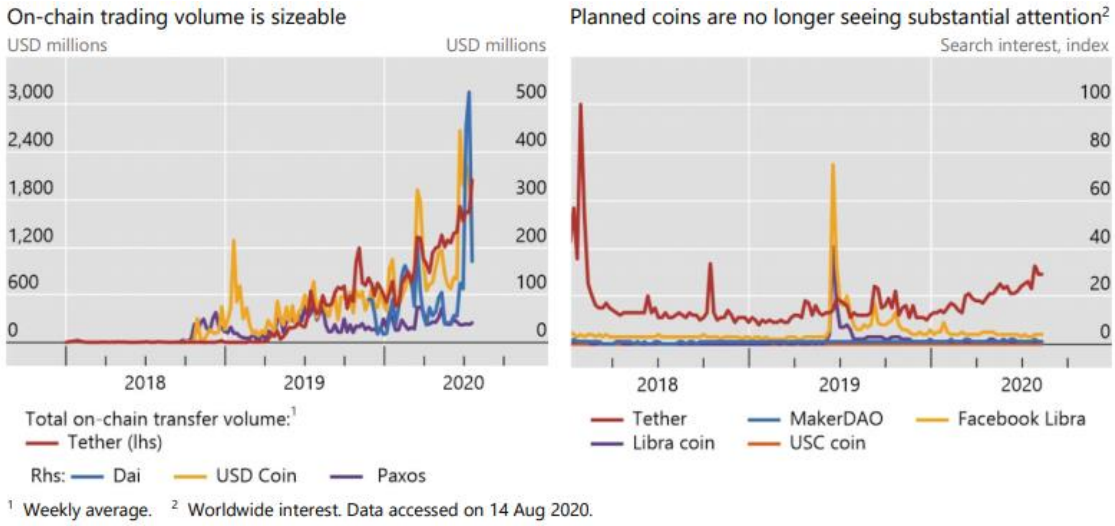
Despite these advantages, cryptocurrencies also face significant disadvantages. One major drawback is the high volatility, prices can vary dramatically, making them risky as both investment and payment tools. Also, the lack of regulations in many countries has exposed companies and individuals to cyberattacks, frauds and other illegal actions. Furthermore, many of these companies that try to get crypto coins by 'mining', use huge amounts of energy that affects the environment, especially in terms of carbon emissions, raising environmental concerns.[4]

2.4- Evaluation of cryptocurrencies and their potential evolution

The area of crypto is continuously changing. Everyday tons of coins are created, and their prices change constantly. Each coin has a project behind which helps with its potential. This project behind and social media news make a place in the market for the coins, in order to get a better acceptance into the society. Right now, lots of coins are accepted and used. As the graph shows the used coins are stablecoins, these coins are more stable than the known meme coins. Another important part of the project is the usability of coins, for example: they are used to make payments between two users, publicly and anonymously by encrypting the wallet of each one. However, there are a lot of other ways to use cryptocurrencies and everyday new

[4]Ciarko, M., Poszwa, G., Paluch-Dybek, A., & Timur, M. C. (2023). Cryptocurrencies as the Future of Money: Theoretical Aspects, Blockchain Technology and Origins of Cryptocurrencies. *Virtual Economics*, *6*(3), 70-93.

ways appear.



[1] Weekly average. [2] Worldwide interest. Data accessed on 14 Aug 2020.

-Security and regulation

Another important point to deal with is the security and regulation of cryptocurrencies. Nowadays crypto is secure if people know how to manage it. Experts, for example, are hardly ever affected by thieves attacking and trying to steal their cryptocurrencies, since they use protocols to minimize the risk of losing their investments. Some examples of protocols used to ensure safety are; using off-line storage solutions like hardware wallets, or researching in depth about the exchange you are about to do to make sure it is safe.

Also crypto has a wide projection because of the decentralization it has, this decentralization makes a volatile market and the possibility of getting scammed.

To sum up, cryptocurrencies are partially a safe way to keep money. Nonetheless, users must acknowledge that their prices may rise and decrease massively.

security and regulatipon in cryptocurrencies - Bing. (s. f.). Bing. https://www.bing.com/images/search?view=detailV2&ccid=vVH37kZa&id=D05BC93DC635BBD46DC0C3CFD2D2485DC8F03EB4&thid=OIP.vVH37kZapiopzNszhGQCeAHaDi&mediaurl=https%3a%2f%2flh3.googleusercontent.com%2f0asjPD_hlLHL1pC3XSQs44nAAqwPEWvoeyV-qHj_014jvwWWp50284JzodRvTzVooKJwxGa59WhkrABVcjdqn8SOUgRaVH0XXT-kgBaKxm3RRHN3FVhoY445S26w6UrOldCoNPOpWWzvmIeTep-

fc6c&cdnurl=https%3a%2f%2fth.bing.com%2fth%2fid%2fR.bd51f7ee465aa62a29ccdb3384640278%3frik%3dtD7wyF1I0tLPww%26pid%3dImgRaw%26r%3d0&exph=766&expw=1600&q=security+and+regulatipon+in+cryptocurrencies&simid=608031099320492164&FORM=IRPRST&ck=0091DAFE459CDC7F14CEAAB0E41233BB&selectedIndex=1&itb=0

-Acceptance

One of the main concerns when dealing with cryptocurrencies is when they will be an accepted medium of transactions by businesses. Since its creation, several companies have pushed forward campaigns to promote such exchanges. Nonetheless, it was only recently when neobanks brought up the idea of a card with which you can operate using your cryptocurrencies and, in that way, pay for goods or a service with them, if the business allows such payment method.[5]

Whilst cryptocurrencies are not fully integrated in today's society, it is true that it has gained lots of recognition, and it has become more common to see people trading with these currencies which means in the near future it might become just another payment method such as PayPal, for example.

-Use

At the beginning the main use of cryptocurrencies used to be to make payments anonymously, but with the appearance of new cryptos and new projects, up until now this has completely changed.

Other uses are:

- Making investments by holding them over long periods of time regardless of the volatility.
- Staking is another investment method based on locking any amount of cryptos for any amount of time in order to obtain a certain interest.
- Promoting projects by gifting coins in the known airdrops.
- Using a specific coin for small contracts and applications (ETH case) or simply to connect IoT and services.

These are many examples of the uses of cryptocurrencies and others will be created following people's needs and project requirements, but everything that can be imagined can be done with them, and they will become a new commonly used currency because the world is continuously changing.

Cryptocurrencies have come a long way and what started with Bitcoin is now a massive number of different cryptocurrencies, blockchains, tokens and innovative ideas that will trace the future of this area of technology.

[5] Fuentes M., V. (2019-06).Adopción de criptomonedas y aplicaciones Blockchain en el sistema financiero. Disponible en https://repositorio.uchile.cl/handle/2250/173531

The current debate regarding the acceptance of cryptocurrencies by the public sector of our society is the actual key to understanding what the future of this new form of money beholds.

What we can be sure about is that blockchain technology will find its own purpose and CBDCs, a variation of cryptocurrencies that is explained further down in the ethics section, will probably be used by public entities sooner or later.

However, the path for Bitcoin, Ethereum and other conventional cryptocurrencies is still unclear, although data suggests that a slow acceptance of this technology is taking place, and the bear market that took place in 2023 had little to no effect in the way cryptocurrencies are seen as a technology with potential to change things for better. As an example, Binance, one of the main cryptocurrency brokers has doubled its daily visits in 2024 and the value of assets of their clients has surpassed 100.000 million dollars for the first time.

Potential evolution of cryptocurrencies encompasses the further development of new consensus protocols like Proof of History, the emergence of new blockchains with innovative new features and tokens, the development of new technologies that allow for a greater acceptance by the general public, the incorporation of cryptocurrencies as an accepted and extended payment method, new legal regulations regarding this currencies, the already mentioned CBDCs and brand new integrations with AI in the near future and with quantum computing in the long term, with the corresponding adaptations that will be necessary regarding the conception of stronger cryptographic algorithms that even quantum computing finds hard to break. These are some of the evolutions we can expect in the future.

2.5- Ethical analysis

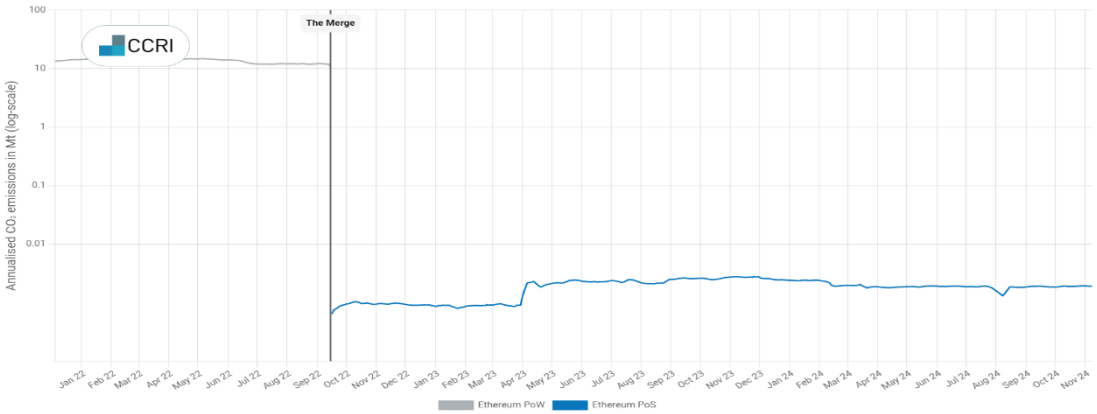
When evaluating the ethics of cryptocurrencies we find that the main debate lies, not in the characteristics and construction of cryptocurrencies themselves, but in the possible uses that this digital currency has and would get to have in case of a possible future expansion. This means that cryptocurrencies don't hold a moral status as such, and it all comes down to what use we make of them. That said, our ethical analysis wants to address whether the difference in ethical use cases vs unethical use cases of cryptocurrencies is enough to justify the support of a hypothetical future expansion in the use of these currencies, considering the inherent characteristics of cryptocurrencies as well. To address the analysis, we are going to evaluate the effect on the political and economic aspects of society, the positive and negative externalities and, lastly, whether cryptocurrencies have a significant responsibility in the facilitation of illegal activity or not.

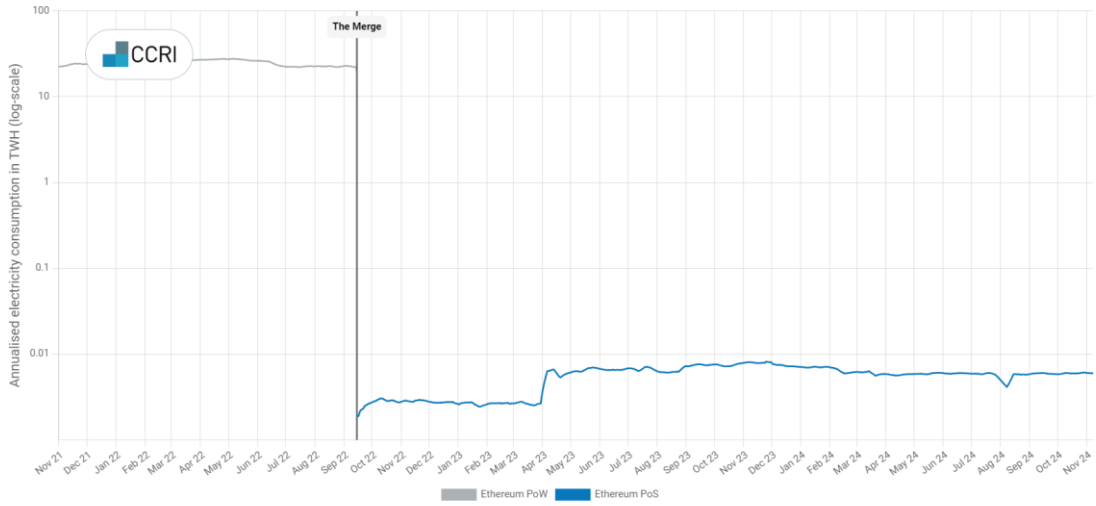
Regarding the political and economic debate, the moral downside that cryptocurrencies face is that, as Tobey Scharding states for the case of Bitcoin: "*The lack of regulation means that Bitcoin's value can fluctuate widely.*"[6] Given that no central power has control over Bitcoin or any other form of cryptocurrency, volatility is increased. This poses a challenge now, in the present, as political regulations by the main nations and a simple tweet from a renowned celebrity like, for example, Elon Musk, can pump or dump the price of Bitcoin and other cryptocurrencies in unforeseeable ways, representing a big risk for users in the present moment, turning cryptocurrencies in a form of volatile investment rather than a stable form of currency. However, we must state that this wouldn't be such a challenge in the case of the adoption of one form of cryptocurrency as the main form of currency, which is similar to the dollar right now. The main form of currency is prone to fewer fluctuations and, additionally, some consensus mechanisms for volatility and offer regulation could be developed in this hypothetical future case, imitating some of the mechanisms that stand behind the way stable coins, those whose value remains unchanged over time, work. Not only that, but addressing the political part of the debate, cryptocurrencies allow a more transparent way of understanding, for example, the use of public money that governments collect, creating a system in which the states transactions with public funds get all written in an immutable and transparent blockchain network that citizens can check in order to know how their taxes are being used, making it difficult for politicians to make use of public funds in corrupt ways. Moreover, if a decentralized currency system was installed, it would reduce the control that governments can have over money, putting obstacles in the way for the development of authoritarian regimes, representing a big upside in terms of achievable liberty.

Regarding the externalities part of the approach, cryptocurrencies, especially those that, like Bitcoin, make use of a Proof of Work consensus mechanism, face a big ethical challenge with the pollution externality, fruit of the massive use of energy these decentralized currencies require to function. Bitcoin's carbon footprint is estimated to be in a range between 22.0 and 22.9 metric tons of CO_2, which would position it between numbers 82 and 83 on the list of biggest emitting countries.[7] Being such a concerning issue, developers are already working on the conceptualization and use of other consensus mechanisms such as Proof of Stake[8]

[6] Scharding, T. (2019). National currency, world currency, cryptocurrency: A Fichtean approach to the Ethics of Bitcoin. *Business and Society Review*, *124*(2), 219-238.
[7] Stoll, C., Klaaßen, L., & Gallersdörfer, U. (2019). The carbon footprint of bitcoin. *Joule*, *3*(7), 1647-1661.
[8] Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: Exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Frontiers in Blockchain*, *6*, 1151724.

with lower energy requirements than PoW. As an example, the following graphs[9] show the decrease in energy consumption and carbon emissions that resulted from the transition from the PoW consensus mechanism to the PoS consensus mechanism in the Ethereum network during the Merge. Consequently, our position regarding this debate is that, although it is a problem now, further development of the cryptocurrency ecosystem in the near future will come with effective solutions that have low energy consumption while achieving the level of security and decentralization that the Proof of Work consensus protocol achieves.





Last but not least, we proceed to evaluate the ethics of cryptocurrencies regarding the facilitation of illegal activity such as money laundering, tax evasion, terrorism financing or commerce of illegal goods and services, among other illegal activities. Bitcoin transactions linked to criminal activity as for 2021 have been estimated to be around 1% of the totality of transactions.[10] The biggest problem with this seemly small 1% is that it represents a growth in the number of illegal transactions in

[9] https://indices.carbon-ratings.com/ethereum-merge
[10] Alfieri, C. (2022). Cryptocurrency and national security. *International Journal On Criminology*, *9*(1), 21-48.

comparison to the past years and, additionally, it doesn't seem to be affected by the price changes in Bitcoin and other cryptocurrencies. For this reason, in our opinion, the ethical debate regarding cryptocurrencies lies in this factor. However, we do not consider this ethical downside to be enough to support a mass prohibition of the use of these kinds of currencies. We believe that, if with further development and adoption of this technology this ethical problem is acknowledged, new innovative solutions that reduce or even make illegal use of these currencies disappear will eventually appear. However, we must point out that, if illegal use of cryptocurrencies keeps expanding and no solutions to the problem arise, cryptocurrency supporters might have to change the approach regarding pseudonymity in this form of digital currency, possibly having to give up this security aspect in exchange for the vanishing of illegal use.

In conclusion, the development of cryptocurrencies is already solving some of the unethical downsides regarding the political and economic situation and the management of negative externalities. Thus, the ethical weak point of cryptocurrencies lies in its use as an illegal payment method, an ethical challenge yet to be addressed that holds by itself the morality of cryptocurrencies.

Conclusions

To conclude, cryptocurrencies are the result of a series of previously developed technologies that have given birth to the form of digital money that could have been expected from the transition to a digital world. Cryptocurrencies have several advantages and disadvantages as has been underlined, however, we must consider that this technology is still evolving and getting integrated into our regulated and centralized economy, finding its place and new possible usages, while bearing in mind the moral implications. We are yet to find the place for cryptocurrencies in our economy, but we are pretty sure that cryptocurrencies are here to stay.

Bibliography

Klarin, A. (2019). The decade-long cryptocurrencies and the blockchain rollercoaster: Mapping the intellectual structure and charting future directions. *Research In International Business and Finance*, *51*, 101067. https://doi.org/10.1016/j.ribaf.2019.101067

View of Cryptocurrencies as the Future of Money: Theoretical Aspects, Blockchain Technology and Origins of Cryptocurrencies. (s. f.). https://www.virtual-economics.eu/index.php/VE/article/view/309/139

What is Cryptocurrency and How Does it Work? (2018, 8 diciembre). /. https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency

Team, I. (2024, 2 junio). *What Are Consensus Mechanisms in Blockchain and Cryptocurrency?* Investopedia. https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp

Lee, J. Y. (2019). A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. *Business Horizons*, *62*(6), 773-784. https://doi.org/10.1016/j.bushor.2019.08.003

https://www.cell.com/heliyon/fulltext/S2405-8440(22)01802-3 Análisis

Sobhanifard, Y., & Sadatfarizani, S. (2019). Consumer-based modeling and ranking of the consumption factors of cryptocurrencies. *Physica A Statistical Mechanics And Its Applications*, *528*, 121263. https://doi.org/10.1016/j.physa.2019.121263

(n.d.). ¿Qué Son Las Criptomonedas? Retrieved November 17, 2024, from

Schmalz, M. (n.d.). *Oxford Blockchain Strategy Programme | Saïd Business*

https://repository.ugc.edu.co/items/44244a00-2aa2-4969-8709-20b54986deaa

School. Saïd Business School. Retrieved November 17, 2024, from https://www.sbs.ox.ac.uk/programmes/executive-education/online-programmes/oxford-blockchain-strategy-programme

Santaella, J. E. (2021, 18 abril). ¿Cómo nacen las criptomonedas? El origen de todo. *Economia3*.https://economia3.com/como-nacen-las criptomonedas/#:~:text=M%C3%A1s%20all%C3%A1%20de%20lo%20que%20mucha%20gente%20piensa,%20el

Bouri, E., Gupta, R., & Roubaud, D. (2018). Herding behaviour in cryptocurrencies. *Finance Research Letters*, *29*, 216-221. https://doi.org/10.1016/j.frl.2018.07.008

Milutinović, M. (2018). *CRYPTOCURRENCY*. Questa Soft. https://www.ceeol.com/search/article-detail?id=695295

La adopción cripto se dispara en 2024: Binance alcanza un crecimiento récord en participación y transacciones de usuarios: Guest Post by Criptotendencias.com | CoinMarketCap. (s. f.). https://coinmarketcap.com/community/es/articles/667ac3f5c6d3433bfb06c6a0/

Research Guides: Fintech: Financial technology Research Guide: Cryptocurrency & Blockchain Technology. (s. f.). https://guides.loc.gov/fintech/21st-century/cryptocurrency-blockchain

(n.d.). ¿Qué Son Las Criptomonedas? Retrieved November 17, 2024, from https://repository.ugc.edu.co/items/44244a00-2aa2-4969-8709-20b54986deaa

Scharding, T. (2019). National currency, world currency, cryptocurrency: A Fichtean approach to the Ethics of Bitcoin. *Business and Society Review*, *124*(2), 219-238.

Ciarko, M., Poszwa, G., Paluch-Dybek, A., & Timur, M. C. (2023). Cryptocurrencies as the Future of Money: Theoretical Aspects, Blockchain Technology and Origins of Cryptocurrencies. *Virtual Economics*, *6*(3), 70-93.