Advances in Economics and Business Management (AEBM)
p-ISSN: 2394-1545; e-ISSN: 2394-1553; Volume 10, Issue 1; January-March, 2023, pp. 69-73

http://www.krishisanskriti.org/Publication.html

# Cryptocurrency: Risks to Users

**Karan Bindal**

*Class-12*
*Institute-Daly College*
*E-mail: karanbindal00@gmail.com*

**Abstract**—*Cryptocurrency has become more popular in recent years, with 420 million global users estimated in 2023. However, cryptocurrency scams have resulted in losses amounting to billions of dollars for around 50,000 people since 2021. The ease of access and partial anonymity of cryptocurrency makes it a prime target for malicious individuals. This paper explores the vulnerabilities inherent in cryptocurrencies, including partial anonymity, escalating cyber apprehensions, and various schemes that increase the risk to investors. It draws upon secondary research, including governmental reports, articles, and studies, to investigate the dangers of cryptocurrency.*

## 1. INTRODUCTION

With 420 million global cryptocurrency users in 2023, the popularity of Bitcoin, Ethereum, and Tether is constantly increasing. However, not every user would be content with their luck. Since the start of 2021, more than 46,000 people have reported losing over $1 billion in cryptocurrency scams. Crypto has various features that attract scammers and hackers, including the lack of central management and the inability to reverse transactions (Fletcher, 2022).

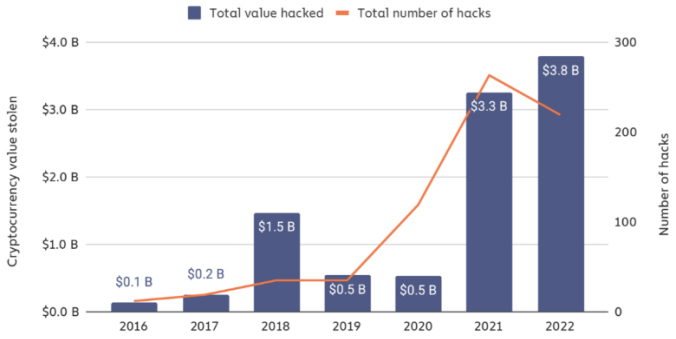


**Figure 1: Total value of and number of hacks from 2016 to 2022 (Team, 2023)**

Of the reported cryptocurrency fraud, most are investment scams. In 2021, the amount of money that hackers and scammers stole was about $680 million, which is six times the money that hackers stole in 2020 (Fletcher, 2022). People aged 20 to 49 were more than three times as likely as older age groups to have reported losing cryptocurrency to a scammer (Ibid). People in their 30s were the hardest hit, with 35% of their reported fraud losses since 2021 being in cryptocurrency (Ibid). Furthermore, the median reported losses for individuals tend to increase with age, topping out at $11,708 for people in their 70s (Ibid). Recognizing the increasing trend of cryptocurrency scams, this paper deliberates on numerous features of cryptocurrency which increase the potential risks its users face.

Aiming to investigate the dangers of cryptocurrency, this paper focuses on the causes and effects of cryptocurrency's weaknesses. The paper consists of secondary research, including various sources like other published research papers, news articles, government reports, and surveys. While mainly focussing on Bitcoin, the paper also takes into account other cryptocurrencies like Ethereum. In this paper, the weaknesses of cryptocurrency are divided into four main categories which cover various aspects and perspectives of the hardships that investors face. The paper argues that partial anonymity, cybersecurity concerns, lack of government recognition, and frequent scams make cryptocurrency a high-risk investment for its users.

## 2. PARTIAL ANONYMITY

Partial anonymity, in its true sense, means that the user/customer only fragmentarily reveals their identity or only reveals their identity to a limited audience. With recent technological advancements, preventing a rival individual/firm from grasping private company information is almost impossible. It has become more accessible to hack into rival firms' databases to gain personal/professional data. This has slowly made its way into Bitcoin as well. It is as easy for scammers and hackers to gain information or access to crypto wallets. This detrimental role has created a domino effect leading people to ask: Is Bitcoin really anonymous? The question shifts to a more controversial one, i.e. is it at least partially anonymous? (Adan, 2023). This is because Bitcoin tells investors that it is anonymous; however, if this is false, it would lose a majority of them, and hence it has to prove to be partially anonymous to stop users from leaving it.

To some extent, Bitcoin does support anonymity. However, it is likely that it could be traced and is also completely transparent. The fundamental feature of cryptocurrency is that it allows the user to have a crypto address that does not reveal their real-world identity. Conversely, a pivotal aspect of

cryptocurrency must be considered to evaluate its capability for anonymity – purchasing. Purchasing is hardly anonymous since cryptocurrency platforms employ know-your-customer (KYC) protocols, for which government-issued ID proofs like a driver's license, Aadhar card, or passport is required to prove one's legal identity. Some platforms may even require users to prove that they have an income source or assets. One reason why platforms are employing KYC protocols is government crackdowns on digital platforms that can be used by criminals to launder money (Adan, 2023). By confirming the identity of a customer, KYC aims to prevent illegal activities such as money laundering, terrorist financing, and tax evasion (Veriff, 2023).

Furthermore, one system that plays a significant role in anonymity is blockchain. It is a public and decentralized register that stores transactions, especially those made in cryptocurrency (*Synopsys*, n.d.). These records are ordered and hence called blocks. These blocks are linked with cryptography and contain a cryptographic hash of the previous block, a timestamp, and transaction data (Ibid). The blockchain allows for the anonymity of transactions, but because this is only partial anonymity, it also poses a risk of traceability that could expose the real identity of the blockchain members involved in the transaction (De Haro-Olmo, Varela-Vaca,& Álvarez-Bermejo, 2020). As a result, cryptocurrencies do not offer sufficient confidentiality to guarantee crypto asset users' privacy rights (Adan, 2023).

## 3. CYBERSECURITY CONCERNS

Cryptocurrency has attracted hackers since its birth in January 2009 because of its untraceable activity. These scammers typically attempt to gain access to individual accounts and then steal private keys, gaining access to people's cryptocurrency wallets. Many of these cryptocurrencies work on blockchain technology – a set of blocks with a set of independently verified transactions. Even though this is secure, the private keys are susceptible to theft. To avoid any cybersecurity difficulties, it is vital to understand how investing in cryptocurrency can lead to trouble. This section outlines some of the most frequent cybersecurity concerns associated with cryptocurrency investment that one should be aware of (Roohparvar, 2022).

Firstly, illegal trading platforms are a major concern. Because cryptocurrency is still in its infancy and has yet to reach its true potential, new trading platforms are springing up to acquire investors' trust. However, these platforms' initial security is underdeveloped and hence are untrustworthy. One such example is that of One Coin, which was discovered to be a multi-level marketing scam. A hack or data leak is not the only risk linked with cryptocurrency. Fraudulent conduct like this can sometimes take place right in front of the user's eyes. Many other firms are also often sued or accused of operating illegally or having illegal goals or manufacturing processes (Roohparvar, 2022). In another instance, Binance and Coinbase, two of the biggest crypto trading platforms in the world, were accused of operating illegally by the Securities and Exchange Commission (SEC). The agency filed charges against Binance and, in the following days, accused Coinbase of violating securities laws. The SEC accused Binance and Coinbase of operating securities exchanges and selling digital assets that should have been registered. Coinbase made billions of dollars facilitating the sale of crypto assets as an unregistered exchange and depriving investors of significant protections. However, in its lawsuit against Binance, the S.E.C. accused its chief executive, Changpeng Zhao, of civil fraud. Moreover, Binance was accused of funneling billions of dollars of customer money to a company owned separately by Mr. Zhao. The SEC charged Mr. Zhao and the company and accused Binance of about a dozen other violations, including misleading investors about the adequacy of its systems to detect and control manipulative trading (Livni, 2023).

Secondly, the presence of third-party apps also raises concerns about cryptocurrency's secure nature. Investors may use third-party apps, tools, and software to handle their digital assets and wallets. For example, it is common for investors to use crypto tax reporting services, exposing them to additional cybersecurity threats. In 2020, it was reported that a hacker stole data from over 1000 users after breaking into CryptoTrader.Tax. The hacker gained access by entering a marketing and customer service representative's account, which displayed sensitive information that put users at risk (Roohparvar 2022).

Thirdly, the security of an account is a major concern with cryptocurrency users. "Private Keys" is one such feature that helps keep up the integrity of the accounts (Roohparvar 2022). Private keys are long alphanumeric codes that act like passwords and are used to authorize transactions. Their wallets generate a user's private key which is used to create their public key (wallet address) using encryption (Frankenfield, 2023a). Stored chiefly on laptops, they allow access to the accounts quickly. However, this is highly insecure as hackers can easily acquire this key and log into others' accounts. Furthermore, because cryptocurrency is not strictly controlled, there is no way to recover a private key if it is stolen. Today, investing in cryptocurrency is getting riskier and riskier since investors are the only ones responsible for keeping their private keys safe and out of the reach of hackers (Roohparvar, 2022).

Fourthly, cryptocurrencies are decentralized, due to which no agency, government, or organization is responsible for its production, management, or movement, making cryptocurrency exchanges unregulated exchanges (Roohparvar, 2022). One such implication of this is as follows: On a blockchain, there is a constant risk of a 51% attack, which is a situation when a miner or group of them gets more than 50% of the network's mining hash rate control. While in control, an ill-natured group can reverse the completed transaction, pause the transaction in process, double spend coins, prevent new transactions from getting validation

and much more (Tambe, 2023). Nevertheless, cryptocurrency restrictions are expected to be tightened in more nations, as they can attract hackers and scammers (Roohparvar, 2022). This is elaborated on in the next section.

Furthermore, crypto-malware is another significant obstacle. It is a type of malware that allows hackers to mine cryptocurrencies on another external server. Two methods that hackers use to infect someone's computer include deceiving the user into installing malicious code on their laptops using phishing-like tactics. Phishing is an attack that attempts to steal one's money, or one's identity, by getting one to reveal personal information. Malicious code is installed into websites or advertisements by cybercriminals. When victims engage with them, the code is activated, allowing hackers access.

Finally, cryptocurrency's user perplexity is not up to the mark. Because crypto is still a new concept, it can negatively impact investors. Cryptocurrencies, crypto exchanges, and blockchain technology are all complicated by their very nature. Even seasoned investors may find it challenging to comprehend. (Roohparvar, 2022). Moreover, cryptography, the backbone of cryptocurrency, occurs solely in the internet's ether. To explain this further, cryptography is the mathematical and computational practice of encrypting and decrypting data, a technique of sending messages to two or more people after encrypting the data (Seth, 2022). Since Ethernet technology allows devices to be connected to a Local Area Network (LAN), there is some risk in cryptography. Unlike traditional assets such as money in a savings account, cryptocurrency is often less safe and riskier for investors (Roohparvar, 2022).

## 4. LACK OF GOVERNMENT RECOGNITION

With bitcoin whitepaper's (the original thesis paper written in 2008 that helped set the base structure of bitcoin) problems and news, its enthusiasts heralded the cryptocurrency's launch as a new dawn with a new and equitable monetary system (McWhinney, 2022; bitFlyer, n.d.). However, critics believe otherwise. Cryptocurrency plays a significant role in criminal activity and the absence of legal recognition proves that it is "rat poison squared." Signifying that cryptocurrencies are already the hub of criminal activities, the inadequacy of legal tenders makes it even worse (McWhinney, 2022).

One noticeable point is how cryptocurrency has had diverse effects in many parts of the world. Countries like El Salvador have started to use it as a currency but others, like the United States, do not even recognise it as a legal tender (McWhinney, 2022). Australia's treatment of digital currencies meant investors would pay capital gains tax on profits when they sell or trade digital currency through an exchange, and that cryptocurrency would be treated as an asset. (Gould, 2022). Among other things, Bitcoin allows the citizens of a country to undermine government authority by circumventing capital controls imposed on it. It also proliferates illegal activities by helping criminals evade detection. Furthermore, by removing intermediaries, Bitcoin can potentially be a disaster for the current financial infrastructure and may help destabilise it. Government wariness about cryptocurrency can be partly attributed to fear and the lack of transparency about its ecosystem (McWhinney, 2022).

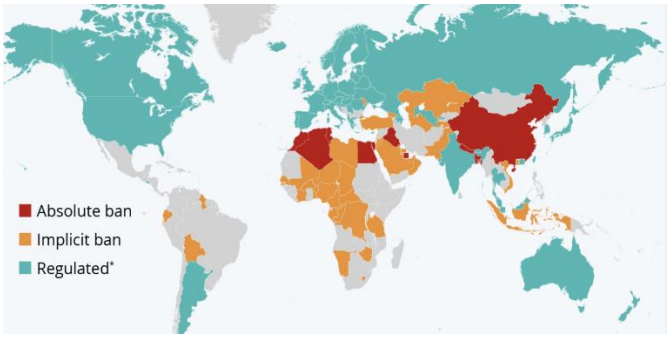


**Figure 2: Government's view on cryptocurrency (Buchholz, 2022)**

Bitcoin has become a touchstone for controversy since it was introduced to the world in the aftermath of the financial crisis, and governments have become more wary, even fearful, of Bitcoin, alternating between criticizing the cryptocurrency and investing in its use for their ends (McWhinney, 2022).

There are several more reasons why governments do not indulge in cryptocurrency. Firstly, it is the lack of awareness of what cryptocurrency really is and how it functions. This is a major obstacle to widespread cryptocurrency adoption. There is an immediate need for awareness of what investors are getting into when investing in digital currency through social media campaigns, advertisements, and word of mouth. Furthermore, cryptocurrencies are also extraordinarily volatile. This dissuades investors from investing in cryptocurrencies. Due to this volatility, investors also face problems in forecasting the probability of the future.

Another problem investors face is the lack of a regulatory framework, meaning there are no rules and regulations that limit the use of cryptocurrencies. There are fewer protection laws for users from financial crime and fraud among investors, hence demoting investors. Finally, cryptocurrencies have uncertainty regarding taxes. Taxes are levied on different cryptocurrencies by governments at different rates. Before investing, potential investors must be aware of the potential tax implication. It is, hence, of the utmost importance for nations to establish transparent taxation laws for cryptocurrencies (Gondek, n.d.). Recapitulating, cryptocurrency represents an international threat to national security worldwide and will soon threaten the financial systems' stability in many. This has resulted in confusion, with different agencies and governments looking at crypto through different lenses and taking different approaches to the issue. Cryptocurrency is a major threat to various financial systems and must be tightly regulated to prevent abuse and instability (Merchant, 2023).

## 5. CRYPTOCURRENCY SCAMS

There are fundamentally two main ways hackers or criminals can gain other individuals' cryptocurrency wallets: directly stealing it or using elaborate schemes to trick people into handing it over themselves. In 2021, crypto criminals and thieves stole a record US$3.2 billion worth of cryptocurrency, an almost fivefold increase from 2020. Moreover, prospects are not looking better. Schemes continue to overshadow outright theft, enabling scammers to lure more and more US$ worth of cryptocurrency annually from unsuspecting victims (Lane, n.d.).

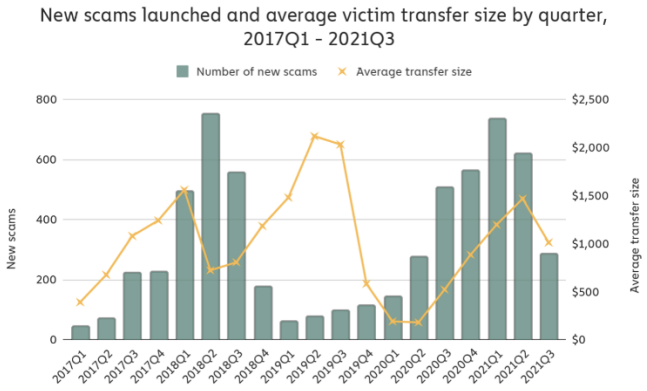


**Figure 3: The rise in the number of scams over the years (Team, 2023)**

Data from the Australian Consumer and Competition Commission confirmed these trends, reporting that more than A$26 million was lost to cryptocurrency scams in 2020 from over 1900 reports. In December 2021, federal police told ABC News that crypto scam losses for 2021 exceeded A$100 million. The actual number is probably higher since many incidents are likely left unreported, often due to victim embarrassment (Lane, n.d.)

There are numerous scams that hackers can use to perform wallet thefts. One of these methods is email phishing. This includes a user receiving random emails from strangers for personal login details in exchange for attractive prizes and rewards like the new iPhone or the AirPods. These login details are then used to steal cryptocurrency from wallets. Moreover, investment scams are also frequent today. During investment scams, hackers and scammers create real-looking investment trading platforms. These are often copies or ripoffs of real business sites or completely new but attractive websites (Lane, n.d.). The main thing these sites use to attract users is fake celebrity endorsements. Additionally, more dedicated hackers would keep following up with phone calls and emails to keep up the facade of a legitimate business. After cryptocurrency deposits are made, users may be able to "trade" on the platform but will not be able to withdraw their earnings. Delay tactics include asking for further deposits to be made for fees or taxes.

Finally, another major scam is the romance scam. The hacker creates fake profiles and matches with users on dating profiles. They may ask for funds due to personal family emergencies or some personal crisis or may encourage the user to trade cryptocurrency and then lead them into an investment scam. Another risk is losing access to the wallet if login credentials are forgotten or a mobile phone linked to the account is lost or stolen. Web-based wallets, such as those offered by Coinbase, may also be vulnerable to hacking if appropriate security measures are not in place (Lane, n.d.).

Scammers and hackers are increasingly getting creative to lure users into traps or make them share their personal information/private keys. For this reason, crypto scams include impersonation of celebrities, huge awards, or carefully modified lies based on the interest of the victim being targeted. Strange emails, texts from people one has just met (online or offline), and constant talks about cryptocurrency with them almost mean the communication is a scam. To save money, the best method is to identify it before it is too late because once a transaction has occurred, the user can consider their financial assets lost (Johnson, 2023).

## 6. CONCLUSION

The weaknesses in cryptocurrency is currently putting off many users worldwide with investment, phishing, romance scams and more. With young adults getting addicted to investing and creating more accounts, scammers/hackers are getting more and easier targets to steal from. Due to the lack of government acknowledgement, the security measures that cryptocurrency has for its users are not up to date and users have suffered many problems that include wallet theft and various scams. With the growing use of cryptocurrency, there is also a growing need for complete anonymity, something that is believed to exist but does not in reality.

The research into the weaknesses of cryptocurrency is of significance as it contributes to the conversation on the consequences of investing in cryptocurrency and how detrimental it can be to unsuspecting investors. The number of scams that currently exist in cryptocurrency is increasing drastically, and this research would help people gain awareness and allow them to familiarize themselves with various aspects of cryptocurrency before they invest.

Future projections of cryptocurrency users are estimated to increase drastically over the next few years. This takes into account past and present numbers. As of 2023, 420 million people use crypto worldwide, and it is projected that by 2027, there will be 994.30 million cryptocurrency users. With these projections, we can predict that the use of crypto will go up with high hopes for these weaknesses to strengthen over time. As a result, governments should mobilize to legislate new laws and regulations that make wallets/accounts safer and restrict scammers and hackers that can prey on the increasing user base (TripleA, 2023).

## BIBLIOGRAPHY


[1] Adan. (2023, January 12). The benefits and risks of anonymity enhanced crypto-assets - Adan. Retrieved from https://www.adan.eu/en/publication/the-benefits-and-risks-of-anonymity-enhanced-crypto-assets/

[2] Ariella, S. (2023). 30 Striking Cryptocurrency Statistics [2023]: Market Value, Bitcoin Usage, and Trends. Zippia. Retrieved from https://www.zippia.com/advice/cryptocurrency-statistics/#:~:text=There%20are%20approximately%20200%2C000%20Bitcoin,in%2C%20or%20traded%20a%20cryptocurrency.

[3] Bainbridge, A., & Kent, L. (2023, January 17). Cryptocurrency scams targeting Australians as scammers bank more than $100 million. ABC News. Retrieved from https://www.abc.net.au/news/2021-12-08/cryptocurrency-scams-targeting-australians-losing-millions/100678848?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web

[4] Buchholz, K. (2022, March 18). Where the World Regulates Cryptocurrency. Statista Infographics. Retrieved from https://www.statista.com/chart/27069/cryptocurrency-regulation-world-map/

[5] Content, S. (2022, April 28). Is Bitcoin Truly Anonymous? Marin Independent Journal. Retrieved from https://www.marinij.com/2022/04/27/is-bitcoin-truly-anonymous/#:~:text=To%20some%20extent%2C%20Bitcoin%20is,reveal%20your%20real%2Dworld%20identity.

[6] Darah, D. (2021). What's the difference between internet and Ethernet? Networking. Retrieved from https://www.techtarget.com/searchnetworking/feature/Whats-the-difference-between-internet-and-Ethernet#:~:text=Ethernet%20is%20a%20technology%20that,to%20talk%20to%20each%20other.

[7] De Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. Sensors, 20(24), 7171. https://doi.org/10.3390/s20247171

[8] Desjardins, J. (2018, March 20). The Rising Problem of Crypto Theft, and How to Protect Yourself. Visual Capitalist. Retrieved from https://www.visualcapitalist.com/problem-crypto-theft/

[9] Desjardins, J. (2018b, March 20). The Rising Problem of Crypto Theft, and How to Protect Yourself. Visual Capitalist. Retrieved from https://www.visualcapitalist.com/problem-crypto-theft/

[10] Fletcher, Emma (2022, August 11). Reports show scammers cashing in on crypto craze. Federal Trade Commission. Retrieved from https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze

[11] Frankenfield, J. (2023). What Is Bitcoin? How to Mine, Buy, and Use It. Investopedia. Retrieved from https://www.investopedia.com/terms/b/bitcoin.asp

[12] Frankenfield, J. (2023b). Private Key: What It Is, How It Works, Best Ways to Store. Investopedia. Retrieved from https://www.investopedia.com/terms/p/private-key.asp#:~:text=How%20Do%20Private%20Keys%20Work,your%20wallet%20address

[13] Gondek, C. (n.d.). 10 Main Challenges of Crypto Adoption. OriginStamp. Retrieved from https://originstamp.com/blog/10-main-challenges-of-crypto-adoption/

[14] Gould, C. (2022, October 26). Major crypto change hidden in budget. News. Retrieved from https://www.news.com.au/finance/economy/federal-budget/major-crypto-change-hidden-in-federal-budget/news-story/51c3972e4c29b731fff4320e1c10e5c1

[15] Johnson, H. (2023, May 31). What Are the Most Popular Crypto Scams to Watch For in 2023 · TIME Stamped. TIME Stamped. Retrieved from https://time.com/personal-finance/article/popular-crypto-scams/

[16] Lane, A. M. (n.d.). Crypto theft is on the rise. Here's how the crimes are committed, and how you can protect yourself. The Conversation. Retrieved from https://theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027

[17] Livni, E. (2023, June 7). Crypto Crackdown: Coinbase and Binance Lawsuits Shake Markets. The New York Times. Retrieved from https://www.nytimes.com/2023/06/07/business/sec-lawsuit-crytocurrency-explainer.html

[18] McWhinney, J. (2022). Why Governments Are Wary of Bitcoin. Investopedia. Retrieved from https://www.investopedia.com/articles/forex/042015/why-governments-are-afraid-bitcoin.asp

[19] Merchant, M. (2023, March 9). The Shocking Truth About Crypto: Why Governments Are Terrified Of Decentralized Networks. Benzinga. Retrieved from https://www.benzinga.com/markets/cryptocurrency/23/03/31277641/the-shocking-truth-about-crypto-why-governments-are-terrified-of-decentralized-networks Partial Anonymity. (n.d.). Retrieved from https://www.freehaven.net/paper/node7.html

[20] Reeves, P., Shen, E., & O'Grady, R. (n.d.). Global Legal Insights: Blockchain & Cryptocurrency Regulation 2023. Global Legal Insights. Retrieved from https://www.gtlaw.com.au/knowledge/global-legal-insights-blockchain-cryptocurrency-regulation

[21] Roohparvar, R. (2022). The Cybersecurity Risks of Cryptocurrency. Cyber Security Solutions, Compliance, and Consulting Services - IT Security. Retrieved from https://www.infoguardsecurity.com/the-cybersecurity-risks-of-cryptocurrency/

[22] Seth, S. (2022). Explaining the Crypto in Cryptocurrency. Investopedia. Retrieved from https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/

[23] Statista. (n.d.). Cryptocurrencies - Worldwide | Statista Market Forecast. Retrieved from https://www.statista.com/outlook/dmo/fintech/digital-assets/cryptocurrencies/worldwide#:~:text=In%20