Security of Modern Cryptocurrencies

Cryptocurrencies have become very popular in the last decade. On a theoretical level, all of them rely on the block chain systems. However, they have different implementations and most of the time they are overlooked. Security implications are among these implementations that are not inspected close enough in cryptocurrencies. A reason for this is because block chain technology makes the data immutable. This does not mean that in order to interact with system, an application is not required. The implementation of these applications differentiates and that is where the security concerns arise. There has been many studies and discussions about cryptocurrencies and block chain technology. One of the topics of discussion that will be covered in this essay is the cryptocurrency network analysis. The study of block chain network can suggest the possible future malicious activities and detection of fraud attempts in the network. Another topic of discussion of this essay is the security implementations of specific cryptocurrency systems and their evaluation. For this purpose, Monero and Zcash will be subject to study as they are claimed to be more secure than mainstream options such as Bitcoin or Ethereum. Finally, as mentioned before, mathematical theory of block chain systems is considered to be secure but the implementations of applications create a security exploits.

Cryptocurrency was introduced by a programmer called Satoshi Nakamoto, whose actual identity has never been verified. Therefore, there is no single person known to be responsible for the creation of Bitcoin. In the ground-breaking 2008 paper, "Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto proposes a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without involving a financial institution (Nakamoto, 2008). This system leverages digital signatures and solves the double-spending problem using a peer-to-peer network, which timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work. This forms a record that cannot be altered without redoing the proof-of-work, ensuring the security and integrity of the system (Nakamoto, 2008). One of the main strengths of cryptocurrencies, as highlighted by Nakamoto's proposal, is the elimination of the need for trust in financial institutions or third parties. The peer-to-peer network is designed to be robust in its unstructured simplicity, with nodes working simultaneously with minimal coordination (Nakamoto, 2008). This setup allows for a decentralized system where nodes can leave and re-join the network at will, accepting the longest proof-of-work chain as evidence of the events that transpired during their absence (Nakamoto, 2008). Additionally, the system ensures that as long as the majority of CPU power is controlled by honest nodes, they will generate the longest chain and outpace any potential attackers, maintaining the security of the network (Nakamoto, 2008). Nodes vote with their CPU power to express their acceptance of valid blocks and rejection of invalid ones, making it possible to enforce any necessary rules and incentives through this consensus mechanism (Nakamoto, 2008). In conclusion, Nakamoto's innovative proposal of a decentralized electronic cash system, which later became Bitcoin, introduced the world to the concept of cryptocurrencies. This system provides significant advantages, such as eliminating the need for trust in financial institutions, creating a robust and secure network, and offering a consensus mechanism for enforcing rules and incentives. Bitcoin was the first cryptocurrency that was introduced, and its price was zero dollars. After two years it was released, in February of 2011, Bitcoin finally reached the value of one dollar. From this point on, according to Ho et al. (2020), Bitcoin has dominated the market until 2016, meanwhile other cryptocurrencies were being developed adopting the block chain technology. Ho et al. (2020) also states that after mid-2017, Ethereum and it strongly correlated cryptocurrencies such as Cardano (ADA), NEO, and OMG which share the feature of using smart contracts to automatically execute business functions have replaced Bitcoin in the ranking tables. In addition, Ho et al. (2020) also derive the conclusion from their research that during the Coronavirus outbreak in 2019, QTUM and Binance coin (BNB) has been close in on the rivalry for the leadership with Ethereum. Since from the beginning the cryptocurrencies are believed to be secure and private. Bitcoin was famous for becoming a currency for illegal purchases. The cryptocurrency network, including Bitcoin, is reliable and secure due to the block chain technology, but its privacy is questionable. In his 2015 paper, "Bitcoin: under the hood," Aviv Zohar discusses the myths, hype, and true worth of Bitcoin, shedding light on the strengths of cryptocurrencies and the potential impact of these digital assets on various aspects of our lives (Zohar, 2015). Bitcoin's design fundamentally reimagines money as a social construct, enabling the transmission of value over the internet with the same ease as transmitting information (Zohar, 2015). This disruptive nature of cryptocurrencies holds the promise to transform markets, enable new business models, and affect the ability of governments to control money and regulate businesses (Zohar, 2015). While acknowledging the challenges faced by Bitcoin, Zohar emphasizes the continuous development of innovative solutions to address its shortcomings (Zohar, 2015). The evolution of the Bitcoin protocol and system is influenced not only by its technical strengths and weaknesses but also by social, political, and economic undercurrents (Zohar, 2015). Various stakeholders, including miners, developers, regulators, and adopters, shape the growth and direction of Bitcoin (Zohar, 2015). In conclusion, Zohar's paper highlights the strengths of cryptocurrencies, such as Bitcoin, which have the potential to revolutionize the way we perceive and handle money. By enabling seamless value transmission over the internet, cryptocurrencies can disrupt traditional markets and business models, challenge government control of money, and introduce innovative solutions to overcome existing limitations. As ongoing development continues to expand the potential applications of Bitcoin and other cryptocurrencies beyond the financial domain, these digital assets may come to have a profound impact on our lives (Zohar, 2015). In their 2013 paper, "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," Tyler Moore and Nicolas Christin examine the weaknesses and risks associated with Bitcoin exchanges, which are vital to the ecosystem for converting between Bitcoins and traditional currencies (Moore & Christin, 2013). Their study reveals that the success of Bitcoin has attracted fraudsters, taking advantage of operational insecurity and transaction irreversibility (Moore & Christin, 2013). They analyze the track record of 40 Bitcoin exchanges established over the past three years, finding that 18 of them have closed, often wiping out customer account balances (Moore & Christin, 2013). Although fraudsters are sometimes to blame, other factors also contribute to the closures. Using a proportional hazards model, Moore and Christin demonstrate that an exchange's transaction volume serves as an indicator of whether it is likely to close (Moore & Christin, 2013). They find that less popular exchanges are more likely to shut down than popular ones (Moore & Christin, 2013). Additionally, their logistic regression analysis reveals that popular exchanges are more likely to suffer security breaches, further highlighting the vulnerability of cryptocurrency exchanges (Moore & Christin, 2013). In conclusion, the paper underscores some significant weaknesses of cryptocurrencies, specifically focusing on the risks associated with Bitcoin exchanges. Investors face numerous challenges, including operational insecurity, transaction irreversibility, and the potential for fraud. The findings indicate that both popular and less popular exchanges are susceptible to closure and security breaches, which can result in significant financial losses for customers. As such, users of cryptocurrency exchanges should be aware of these inherent risks and exercise caution when selecting a platform for trading and storing their digital assets (Moore & Christin, 2013). In their 2014 paper, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," Ittay Eyal and Emin Gün Sirer expose critical weaknesses in the security of the Bitcoin mining protocol (Eyal & Sirer, 2014). The authors challenge the conventional wisdom that the mining protocol is incentive-compatible and secure against colluding minority groups. They argue that the protocol does not effectively incentivize miners to follow the prescribed rules (Eyal & Sirer, 2014). Eyal and Sirer present a "selfish mining" attack in which colluding miners can obtain a revenue larger than their fair share (Eyal & Sirer, 2014). They explain that this attack has serious implications for the stability and decentralization of Bitcoin. Rational miners would be inclined to join the selfish miners, causing the colluding group to grow in size until it becomes a majority (Eyal & Sirer, 2014). When this occurs, the Bitcoin system ceases to function as a decentralized currency Moreover, the authors demonstrate that selfish mining could be feasible for any group size of colluding miners unless certain assumptions are made (Eyal & Sirer, 2014). To address this vulnerability, they propose a practical modification to the Bitcoin protocol that protects the system in the general case (Eyal & Sirer, 2014). This modification prevents selfish mining by pools that control less than 1/4 of the resources, a threshold lower than the commonly assumed 1/2 bound but an improvement over the current situation, where any group size can compromise the system (Eyal & Sirer, 2014). In summary, the paper by Eyal and Sirer highlights significant weaknesses in the Bitcoin mining protocol, particularly the vulnerability to selfish mining attacks. These weaknesses pose a threat to the decentralization and stability of the cryptocurrency. The authors' proposed modification offers a practical solution to address this issue, but the inherent vulnerability underscores the need for ongoing research and development to enhance the security and integrity of cryptocurrency systems. In their 2016 paper, "On the Security and Performance of Proof of Work Blockchains," Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun highlight the weaknesses of cryptocurrencies and present a quantitative framework to analyze the security and performance implications of various consensus and network parameters of Proof of Work (PoW) blockchains (Gervais et al., 2016). The authors emphasize that, although the security of Bitcoin has been thoroughly analyzed, the security guarantees of variant (forked) PoW blockchains have not received much attention in the literature. The paper introduces a novel framework that captures real-world constraints, such as network propagation, different block sizes, block generation intervals, information propagation mechanisms, and the impact of eclipse attacks (Gervais et al., 2016). This framework allows the authors to devise optimal adversarial strategies for double-spending and selfish mining while taking these factors into account. Furthermore, the framework enables the objective comparison of the trade-offs between the performance and security provisions of different PoW blockchain instances (Gervais et al., 2016). For example, the authors find that Ethereum needs at least 37 block confirmations to match Bitcoin's security with six block confirmations, given an adversary with 30% of the total mining power (Gervais et al., 2016). This finding suggests that Bitcoin's blockchain offers more security than Ethereum's blockchain, which rewards miners with uncle rewards and performs uniform tie-breaking for blockchain fork resolutions. Additionally, the results indicate that existing PoW blockchains can achieve a throughput of 60 transactions per second without significantly affecting the blockchain's security (Gervais et al., 2016). In conclusion, the paper by Gervais et al. (2016) reveals the weaknesses of cryptocurrencies, particularly in terms of the security and performance implications of various consensus and network parameters of PoW blockchains. The authors' quantitative framework allows for the objective comparison of different PoW blockchain instances, providing insights that can help merchants, miners, and other stakeholders to make informed decisions based on the security provisions and risks associated with transactions and mining activities. In the paper "A fistful of bitcoins: characterizing payments among men with no names," Meiklejohn et al. (2013) explore the unique characteristic of Bitcoin, where the ownership of money is implicitly anonymous, but its flow is globally visible. The authors emphasize the growing gap between the potential anonymity available in the Bitcoin protocol design and the actual anonymity currently achieved by users. To minimize the risks associated with cryptocurrencies, end users can take several actions based on the findings of this study. The authors developed a new clustering heuristic based on change addresses, allowing them to cluster addresses belonging to the same user and identify major institutions and interactions between them (Meiklejohn et al., 2013). Even though this heuristic is not fully robust in the face of changing behavior, it sheds light on the structure of the Bitcoin economy and the organizations involved. End users can adopt practices that increase their anonymity by understanding these heuristics and altering their behavior accordingly. However, Meiklejohn et al. (2013) argue that completely thwarting their heuristics would require significant effort from the user, which may not appeal to all but the most motivated users, such as criminals. To minimize risk, end users should stay informed about the structure of the Bitcoin economy and the major institutions involved, while also being cautious about the services they interact with (Meiklejohn et al., 2013). Additionally, they can use privacy-enhancing tools and services that strengthen the anonymity of their transactions. However, achieving stronger anonymity guarantees may come at the cost of usability, and users must weigh the trade-offs between increased privacy and ease of use (Meiklejohn et al., 2013). In conclusion, end users can minimize the risks associated with cryptocurrencies by understanding the gaps in anonymity, adapting their behavior to counter clustering heuristics, staying informed about the structure of the Bitcoin economy, and using privacy-enhancing tools and services. While achieving stronger anonymity guarantees may require more effort, it is essential for users to make informed decisions based on their individual needs and risk tolerance. In their paper "A Survey on Security and Privacy Issues of Bitcoin," Conti et al. (2018) provide a comprehensive overview of the security and privacy aspects of Bitcoin, including existing vulnerabilities and potential countermeasures. To minimize the risks associated with cryptocurrencies, end users can take several actions based on the findings of this study. First and foremost, users should educate themselves about the major components and functionality of the Bitcoin system, as well as the underlying technologies such as blockchain and the proof-of-work (PoW) consensus protocol (Conti et al., 2018). A deeper understanding of these elements will enable users to make informed decisions about their transactions and the services they utilize. Furthermore, users should stay updated on the latest security threats and vulnerabilities in the cryptocurrency ecosystem and take proactive measures to protect themselves. As the authors emphasize, user privacy and anonymity remain significant concerns in the Bitcoin system (Conti et al., 2018). To address these issues, end users can adopt privacy-preserving solutions that have been proposed in the literature. For instance, users can use anonymizing networks, mixers, or other cryptographic techniques to enhance their privacy and anonymity when conducting transactions. In addition to implementing existing security solutions, users should actively contribute to the development and adoption of more robust and practical security measures for the cryptocurrency space (Conti et al., 2018). This can be achieved by engaging with the research community, participating in discussions, and supporting projects that aim to improve the security and privacy of cryptocurrencies. In conclusion, end users can minimize the risks associated with cryptocurrencies by staying informed about the technology, adopting privacy-preserving solutions, and actively participating in the development of more secure and privacy-enhancing measures. By addressing the critical open challenges and working towards stringent security and privacy solutions, users can contribute to a more secure and private cryptocurrency ecosystem (Conti et al., 2018). As every network does, cryptocurrency networks have entry points and Biryukov & Tikhomirov (2019) explore this idea in their study. They make an attempt to deanonymize any target’s location data by following through the nodes in the network and end up creating an approximate geographical location of the target. The implementation of their tool consists of and is tested on four cryptocurrencies: Bitcoin, Zcash, Dash, and Monero. Bitcoin, most likely being the most famous one, some of these are privacy-focused on their advertisement and require more defence against network analysis, as currently they do not guarantee providing strong privacy guarantees proven by the study. Zcash has a feature that is optional to add a privacy layer called shielded transactions, done by shielded addresses. Quesnelle (2017) explains privacy through zero knowledge proof. Quesnelle (2017) underlines that Zcash is a fork of Bitcoin and as mentioned in the last research studied, coins transferred between source and destination in Bitcoin’s transparent ledger can be traced by third parties who listen to the network. It is only completely secure when a shielded transaction takes place between two shielded addresses, claims Quesnelle (2017). In addition, it is also mentioned that this security measure requires a certain amount of additional computation and takes around 30 seconds to a minute for a single transaction as stated. However, it is also stated that this optional method is not involved in the majority of Zcash transactions, unknown whether it is because of the additional computation time or some other reason. Another brand that improves the security of the like of Bitcoin is Monero (XMR). Monero is based on CryptoNote, which is an electronic cash system explained by Saberhagen (2013) that had the means to improve Bitcoin’s deficiencies, even though their claim was not to replace Bitcoin entirely. However, security was not one of the major focuses that Saberhagen discussed in this paper, even though a section takes place to explain linkability, exculpability, unforgeability, and anonymity. These were not specified in relation to Bitcoin, declaring whether they are different or not and if they are, how different. Developers of Monero have taken CryptoNote as a base concept and built over it with RandomX to validate transactions with proof of work in order to create a more private network compared to Bitcoin. Unlike Bitcoin, the ledgers and transactions were no longer transparent in Monero, even though they were still decentralized and public. Monero’s transaction details were obfuscated, keeping user addresses, wallet balances and all transaction details private, which has created an interest for the community with malicious intent. According to CNBC, in the first half of 2018, Monero was used in 44% of cryptocurrency ransomware attacks. The users were allowed to share their private view key but for Monero it was enforced by the system use the security implications such as Zcash’s where zero knowledge proof method protects the addresses and transactions of users, as well as using decoy outputs to obfuscate a user’s outputs in the network. Kfir (2018) highlights the potential risks that cryptocurrencies pose to national security, particularly with regard to terrorism financing. The study focuses on understanding the nature of cryptocurrencies, how criminals exploit them, and how terrorists could potentially leverage digital currencies for their illicit activities. A key issue identified in the paper is the absence of an international regulatory regime that clearly defines cryptocurrencies and provides guidance on how to regulate the sector effectively (Kfir, 2018). The author emphasizes the need for national, regional, and international measures specifically tailored to address the unique characteristics of cryptocurrencies, rather than merely adapting existing regulations designed for fiat money (Kfir, 2018). Kfir (2018) also underscores the importance of training law enforcement and security institutions to better understand cryptocurrencies and encouraging people to report scams or thefts. The study suggests that the cryptocurrency insurance market has emerged to address some of these concerns, providing traditional services such as theft protection and coverage for service interruptions. Kfir (2018) also acknowledges that certain cryptocurrencies, like Monero and PIVX, are designed to be harder to trace due to their cryptographic structures. Addressing these coins without undermining their appeal to potential users requires fostering a know-your-customer ethos and promoting due diligence among virtual currency exchanges (Kfir, 2018). Lastly, the author points out that the increasing popularity of cryptocurrencies stems from growing disillusionment with traditional state systems and financial institutions. As a result, many people are drawn to cryptocurrencies and anonymity-enhancing technologies like Tor (Kfir, 2018). The paper concludes that striking a balance between encouraging technological innovation and appropriately regulating these technologies is essential to prevent their exploitation for nefarious purposes (Kfir, 2018). Weichbroth et al. (2021) provide an extensive analysis and review of the recent literature on the security of cryptocurrencies, focusing on both technology-oriented solutions and human-related factors. The authors acknowledge that neither aspect is currently robust or mature enough to eliminate security issues. According to a report from Trail of Bits, the immutability of distributed ledger technology (DLT) can be compromised by subverting blockchain implementations, networking, and consensus protocols (Weichbroth et al., 2021). Additionally, the authors point out that human error accounts for 95% of security system failures (Weichbroth et al., 2021). The study highlights the need for user education and training, as well as the development of software systems and tools, which may incorporate artificial intelligence-based defense techniques, to address these security challenges (Weichbroth et al., 2021). The increasing interest from governments and central banks in exploring central bank digital currencies (CBDCs) underscores the importance of addressing cybersecurity and privacy concerns on a national scale (Weichbroth et al., 2021). The authors identify three main varieties of digital currencies: cryptocurrencies, stablecoins, and central bank digital currencies (CBDCs). Security remains a crucial aspect for all these digital currencies, including protection against double-spending, counterfeiting, and account and data breaches (Weichbroth et al., 2021). The authors believe that new payment systems with recent technological advancements will benefit businesses and individuals in terms of trust, regulatory stability, and audit transparency (Weichbroth et al., 2021). Furthermore, systematic development of users' security awareness through education, training, and testing will help mitigate risks and threats. Weichbroth et al. (2021) suggest that future research should focus on developing proactive cybersecurity risk mitigation strategies that cover prevention, detection, and remediation issues in order to better address the security concerns surrounding digital currencies. Navamani (2021) provides an extensive review of security and privacy aspects related to cryptocurrencies, with a particular focus on Bitcoin. The author acknowledges that the rapid growth in the market assessment of cryptocurrencies has led to adversaries exploiting deficiencies for profit. The study delves into cryptocurrency protocols, their usefulness, and the interactions within the system (Navamani, 2021). Bitcoin, one of the most popular cryptocurrencies, attracts both enthusiasts interested in the decentralized blockchain concept and individuals seeking to exploit the blockchain interconnections for malicious purposes (Navamani, 2021). The author explains that the decentralized nature of Bitcoin and its consensus mechanisms, such as Proof of Work (PoW), ensure that every user agrees on a transaction, thereby enhancing security. However, these same features can create loopholes that are exploited by malicious actors (Navamani, 2021). Navamani (2021) discusses various attacks that can affect Bitcoin and provides countermeasures to address them. While existing research has explored different ways to mitigate and deal with some cyberattacks, no procedure can guarantee the total security of Bitcoin and the blockchain's secure functioning (Navamani, 2021). The decentralized concept of the blockchain has raised privacy concerns and issues related to anonymous users (Navamani, 2021). In summary, Navamani's (2021) review article highlights the privacy and security problems in various areas of cryptocurrency, focusing on Bitcoin's architecture and workings. The study examines the privacy and security issues that can arise at different stages of transactions, from their creation to their addition to the blockchain (Navamani, 2021). The author emphasizes the need for further research on individual and anonymous user privacy concerns in the rapidly growing world of cryptocurrencies, as well as addressing security challenges in the Bitcoin network (Navamani, 2021). This work aims to inspire researchers to explore this intriguing domain further. Bucko, Paľová, and Vejačka (2015) explore the phenomenon of cryptocurrencies, digital currencies based on the principles of cryptography. While Bitcoin is often confused as the only cryptocurrency, the authors highlight the emergence of various other cryptocurrencies with similar underlying principles. They emphasize the benefits of using cryptocurrencies, such as low fees, the ability to make virtually anonymous payments without involving banks, and an expected high level of protection for personal data. However, they also point out the main disadvantages, including high volatility, e-wallet thefts, and the potential for funding anonymous criminal activities. The paper investigates the security of cryptocurrency mining, holding, and transferring, and discusses the fundamental arrangements required for building trust in cryptocurrencies (Bucko et al., 2015). Their research identifies multiple interconnected factors affecting trust in cryptocurrencies, which in turn influence their usage. Enormous volatility in cryptocurrency exchange rates presents a high trading risk and contributes to the formation of price bubbles (Bucko et al., 2015). Despite attracting many speculators, the authors argue that cryptocurrencies struggle to retain their value, leading to a potential shift in perception from payment medium to specific commodities. While cryptocurrencies have the advantage of easy portability due to their virtual nature, they remain unusable outside electronic environments (Bucko et al., 2015). Cryptocurrencies are still popular in the black economy, and the authors suggest that if trust in cryptocurrencies increases among potential legitimate users, they will likely see broader, official adoption (Bucko et al., 2015). However, if trust does not reach the necessary levels, the cryptocurrency boom may subside. To increase security and trust in the industry, the authors recommend that regulators worldwide create and enforce standards regarding cryptocurrency use (Bucko et al., 2015). In their 2018 paper, Francés, Grau-Carles, and Arellano examine the characteristics of daily price series for 16 different cryptocurrencies between July 2017 and February 2018. They utilize the Minimum Spanning Tree (MST) and hierarchical analysis through dendrogram methodologies, both derived from Pearson correlations between daily returns, to visualize market relationships between the analyzed assets. Their findings reveal a high correlation between price movements across all the currencies studied (Francés et al., 2018). Interestingly, the authors identify Ethereum (ETH) as a benchmark currency in the cryptocurrency market, rather than the more popular and higher trading volume cryptocurrency, Bitcoin (BTC) (Francés et al., 2018). The MST places Ethereum in a central position in the network, with Bitcoin appearing in one of the branches. Furthermore, the cluster analysis using the dendrogram supports this conclusion, placing Bitcoin in a different cluster from the one obtained with ten other currencies (Francés et al., 2018). The results of this study offer a novel approach to analyzing cryptocurrency behavior through network analysis using Pearson correlations. The network obtained serves as a useful tool for understanding the interrelationships between the financial assets involved (Francés et al., 2018). These findings could prove valuable for investors when making portfolio decisions, particularly considering that the correlation between financial assets is fundamental to portfolio optimization theory.

In conclusion, cryptocurrencies have revolutionized the financial landscape by offering decentralization, increased accessibility, and reduced transaction costs. However, they also present significant challenges in terms of security, privacy, and anonymity. The body of literature examined in this essay highlights the strengths and weaknesses of cryptocurrencies and their underlying technologies, shedding light on potential threats and vulnerabilities that end users must be aware of. By understanding these challenges and adopting best practices, users can minimize risks and ensure the safe and secure use of cryptocurrencies. As the cryptocurrency ecosystem continues to evolve, it is essential for both researchers and end users to stay informed about developments in security and privacy to maintain trust and confidence in this transformative technology.

References:

Biryukov, A., & Tikhomirov, S. (2019). Deanonymization and linkability of cryptocurrency transactions based on network analysis. 2019 IEEE European Symposium on Security and Privacy (EuroS&P). https://doi.org/10.1109/eurosp.2019.00022

Bucko, Jozef & Palová, Dana & Vejačka, Martin. (2015). Security and Trust in Cryptocurrencies.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452. https://doi.org/10.1109/COMST.2018.2842460

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In International Conference on Financial Cryptography and Data Security (pp. 436-454). Springer. https://doi.org/10.1007/978-3-662-45472-5\_28

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 3-16). https://doi.org/10.1145/2976749.2978341

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of cryptocurrencies in Blockchain Technology: State-of-art, challenges and future prospects. Journal of Network and Computer Applications, 163, 102635. https://doi.org/10.1016/j.jnca.2020.102635

Guo, X., & Donev, P. (2020). Bibliometrics and network analysis of Cryptocurrency Research. Journal of Systems Science and Complexity, 33(6), 1933–1958. https://doi.org/10.1007/s11424-020-9094-z

Ho, K.-H., Chiu, W.-H., & Li, C. (2020). A network analysis of the cryptocurrency market. 2020 IEEE Symposium Series on Computational Intelligence (SSCI). https://doi.org/10.1109/ssci47803.2020.9308282

Kfir, I. (2020). Cryptocurrencies, National Security, crime and terrorism. Comparative Strategy, 39(2), 113–127. https://doi.org/10.1080/01495933.2020.1718983

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 Conference on Internet Measurement Conference (pp. 127-140). https://doi.org/10.1145/2504730.2504747

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In International Conference on Financial Cryptography and Data Security (pp. 25-33). Springer. https://doi.org/10.1007/978-3-642-39884-1\_3

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

Navamani, T. M. (2021). A review on Cryptocurrencies Security. Journal of Applied Security Research, 18(1), 49–69. https://doi.org/10.1080/19361610.2021.1933322

Pilar, G.-C., Jaureguizar Arellano, D., & Jaureguizar Francés, C. (2018). The cryptocurrency market: A network analysis. ESIC MARKET Economic and Business Journal, 49(3). https://doi.org/10.7200/esicm.161.0493.4i

Weichbroth, P., Wereszko, K., Anacka, H., & Kowal, J. (2023). Security of cryptocurrencies: A view on the state-of-the-art research and current developments. Sensors, 23(6), 3155. https://doi.org/10.3390/s23063155

Yue, Y., Li, X., Zhang, D., & Wang, S. (2021). How cryptocurrency affects economy? A network analysis using bibliometric methods. International Review of Financial Analysis, 77, 101869. https://doi.org/10.1016/j.irfa.2021.101869

Zohar, A. (2015). Bitcoin: under the hood. Communications of the ACM, 58(9), 104-113. https://doi.org/10.1145/2701411