INTERNATIONAL JOURNAL OF FINANCIAL ECONOMICS (IJEFE) e-ISSN: 3063-3648
Vol. 2 No. 1 January 2025, page 48-56

SECURITY AND PRIVACY IN CRYPTOVALUTA TRANSACTIONS: AN ANALYSIS OF THE LITERATURE ON BLOCKCHAIN TECHNOLOGY

Gunawan Widjaja
Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Abstract

Blockchain technology has revolutionised many industry sectors, including finance, through the introduction of cryptovaluta. While it offers significant transparency and decentralisation, it also raises serious challenges related to security and privacy. This article analyses the existing literature to evaluate various aspects of security and privacy in cryptovaluta transactions. The transparency of blockchain, while increasing trust, may result in the risk of disclosure of user identity and transaction details. Advanced technologies such as zk-SNARKs and CoinJoin have been developed to address this issue, enabling the scrutiny of transactions without revealing sensitive information. The security of blockchain networks, while inherently robust, remains vulnerable to attacks aimed at individual users and exchange platforms. Digital wallet theft, phishing attacks, and vulnerabilities in smart contracts are some of the significant risks. The article also emphasises the importance of user education to recognise and address these risks. By combining more advanced security technologies with increased user awareness, it is hoped that an optimal balance between transparency, privacy, and security can be achieved in the cryptocurrency ecosystem.
Keywords: Security, Privacy, Cryptovaluta Transactions.

Introduction

In recent years, the world has witnessed a significant increase in the application of blockchain technology and the use of cryptocurrencies. Cryptocurrencies, such as Bitcoin and Ethereum, have become an important means of exchange, offering a decentralised alternative to the traditional financial system. The technology behind these cryptocurrencies, namely blockchain, not only paves the way for transparent and efficient transactions, but also presents new opportunities in various applications in other sectors such as supply chain, healthcare, and smart contracts (Muciaccia & Lopopolo, 2022)

By utilising blockchain, every step in the supply chain process can be tracked transparently and efficiently, from raw materials to finished products. This enables the tracking of product origins, which is essential for ensuring authenticity and reducing the risk of counterfeit products. In addition, the transparency offered by blockchain helps reduce operational costs, minimise human error, and increase trust between all parties involved in the supply chain (Victor, 2021) .

In the healthcare sector, blockchain can improve the security and integration of medical data, and strengthen patient privacy. Blockchain-based platforms enable

decentralised and secure storage of medical records, as well as controlled access for various healthcare providers, thereby reducing the risk of data breaches and improving the efficiency of care (Iovane & Rapuano, 2021) . In addition, the concept of smart contracts in blockchain presents new opportunities for automation of administrative processes, such as insurance claims, which can be processed automatically without human intervention. Thus, the healthcare industry can become more transparent, efficient and secure, with faster processing times and better managed resources (Agdere, 2024)

However, behind the various benefits offered by blockchain technology and cryptovaluta, there are major challenges related to security and privacy. Digital transactions, especially cryptocurrency transactions, are vulnerable to various forms of security threats such as hacking, fraud, and cyberattacks. Cases of crypto theft amounting to billions of dollars have highlighted the vulnerabilities that exist in these systems. In addition, while blockchain claims to provide transparency, user privacy is often a major concern. Transaction information that remains permanently stored in a public ledger can lead to the risk of unwanted tracking and surveillance (Grosemans ., 2022)

The concept of security in blockchain involves various mechanisms such as cryptography, consensus algorithms, and complex programming techniques. Meanwhile, privacy issues require more advanced approaches such as the use of zero-knowledge proofs or even the development of private blockchains that have limited access. Understanding the extent to which these technologies can guarantee security and privacy is critical, given the growing number of users who rely on these technologies for their financial transactions and digital asset storage (Micheletti, 2020) .

This research stems from the need to provide a comprehensive analysis of how blockchain technology addresses security and privacy issues in cryptocurrency transactions. By systematically compiling a literature review, this research seeks to identify the various existing mechanisms, evaluate their effectiveness, and discover the main challenges faced and proposed solutions.

Research Methods

The study in this research uses the literature method. The literature research method, or literature study, is an approach carried out by identifying, evaluating, and interpreting existing research or writings related to the topic to be researched. In this method, researchers collect secondary data sources such as books, journal articles, research reports, and other relevant sources of information (Sanusi, 2015) ; (Wekke, 2020) . The purpose of literature research is to understand the existing knowledge landscape, identify gaps in previous research, seek inspiration from methods that have been applied, and build a theoretical framework that supports new research.

Systematic and comprehensive literature research ensures that researchers have a solid base and complete information to support their hypotheses or research questions (Syafril & Erlina, 2018) .

Results and Discussion

Blockchain Technology in Providing Security for Cryptovaluta Transactions

Blockchain is a cutting-edge technology that forms the backbone behind the security and transparency of cryptocurrency transactions. Essentially, blockchain is a decentralised digital ledger that records all transactions within a cryptocurrency network. Each transaction is encrypted and wrapped in a block, which is then linked chronologically and sequentially to the previous block, forming an immutable chain. This process creates high transparency and security as each block contains a trace of previous transactions, making it almost impossible to falsify data without detection (Veuger ., 2020)

One of the main aspects that ensure security in blockchain is consensus algorithms, such as Proof of Work (PoW) or Proof of Stake (PoS). These algorithms are responsible for validating and confirming new transactions, guaranteeing that all participants in the network agree on the current status of the ledger. PoW, for example, involves solving complex mathematical problems that require large amounts of computing power, making attacks or data manipulation extremely costly and time-consuming. Meanwhile, PoS allows users with a certain amount of cryptovaluta to validate transactions based on their ownership, which also increases the security of the network (Cornelis, 2023) .

In addition to consensus algorithms, cryptographic hashing and digital signature features also strengthen blockchain security. Cryptographic hashing creates a unique fingerprint for each transaction, helping in detecting any unauthorised alteration or manipulation of the data. Digital signatures, on the other hand, ensure that the sender of each transaction can be precisely verified as such, preventing fraud attempts and providing strong authentication. The use of hashes and digital signatures together make blockchain a highly secure and trusted system to facilitate cryptovaluta transactions (Campo, 2021) .

Finally, the decentralised nature of blockchain technology ensures that there is no single point of failure in the system. By distributing the ledger to various nodes in the network, blockchain ensures high redundancy and reduces the risk of centralised attacks (Milan, 2022) . If one node is attacked or fails, other copies of the ledger remain intact and operational, keeping data integrity intact. The addition of these security mechanisms makes blockchain indispensable in today's digital age, securing cryptovaluta transactions in an unprecedented way, while strengthening users' trust in a transparent and secure digital financial system (Macchia & Giugno, 2022) .

Blockchain Technology Addresses Privacy Issues in Cryptocurrency Transactions

Blockchains and cryptocurrencies, such as Bitcoin and Ethereum, are known for offering high transparency in their transactions. However, this transparency can pose challenges regarding user privacy, especially when all transactions and addresses are publicly visible in the ledger. To address this issue, some blockchain technologies have developed advanced privacy features, one of which is the use of pseudonymous addresses. Although the real identity is not directly associated with these addresses, transaction activity can still be traced if someone is able to associate the address with the user's identity, posing privacy challenges that must be addressed (Aalders, 2023) .

One solution to enhance privacy in blockchain is the use of zero-knowledge proof (ZKP) technology. ZKP allows one party to prove to another party that they are aware of information without revealing the information itself. In the context of blockchain, this technology can be used to validate transactions without revealing sensitive details, such as the amount of funds transacted or the identity of the parties involved. Zcash is one of the cryptovaluta that implements ZKP to offer a higher level of privacy for its users, enabling fully encrypted transactions within the blockchain (Mooij ., 2023)

Another technology that plays an important role in enhancing blockchain privacy is the use of "coin mixing" or "tumbler" transactions. This process involves combining or mixing cryptovaluta from various users before they are redistributed to the destination address. By splitting and mixing transactions from multiple sources, this technique makes it more difficult to trace the origin and destination of individual transactions. Monero, a cryptocurrency that emphasises privacy, uses such techniques alongside methods such as ring signatures and stealth addresses to disguise transactions and hide the identity of senders and recipients (Mintas ., 2023)

In addition to these technological innovations, some blockchain projects are developing smart contract platforms that offer further privacy options. On these platforms, users can customise the level of transparency of their transactions and interactions as needed. This allows decentralised applications (dApps) to cater to users with different privacy needs without compromising security and trust. As technologies and strategies to address privacy issues on blockchain continue to evolve, users can have greater confidence in keeping their personal information private and secure in the crypto ecosystem (Callens, 2021) .

Beyond the technologies already mentioned, further development is being done on various protocols and standards that support privacy. One example is Mimblewimble, which is a blockchain protocol that enables more anonymous and efficient transactions by hiding transaction amounts and addresses. Grin and Beam are two cryptovaluta that utilise this protocol to provide an additional layer of privacy. Additionally, projects such as Aztec and StarkWare are exploring the use of Zero-Knowledge Rollup (zk-Rollup) technology on the Ethereum blockchain to create

scalable privacy solutions without compromising network speed and efficiency (Sabry, 2021) .

Another concept that is gaining popularity is the use of Layer 2 networks to enhance privacy on top of the main blockchain. Bitcoin's Lightning Network, for example, plays an important role in processing transactions off-chain before completing the main transaction on the blockchain, thus ensuring a higher level of privacy as not all transactions are visible on the main ledger (Sartori, 2020) . Additionally, projects such as Raiden Network are developing similar solutions for Ethereum, improving efficiency and privacy in the crypto ecosystem as a whole.

Regulation also plays an important role in blockchain privacy issues. While maintaining a level of anonymity, there needs to be a balance to ensure that this technology is not misused for illegal activities. Several governments and global regulatory entities are discussing the appropriate policies to oversee the use of privacy technologies in cryptovaluta, so as to provide better security for users without violating existing regulations. User education on the importance of privacy and how to protect their sensitive information is also an important aspect in mitigating the risks arising from blockchain transparency (Lia et al., 2021) .

As such, privacy is a major challenge in blockchain technology, more specifically in the context of cryptocurrency transactions. While the technology offers high transparency, many are innovating to resolve privacy issues without compromising the basic advantages of blockchain. Technologies such as zero-knowledge proof, coin mixing, and customisable smart contracts are being studied and implemented to enhance user privacy. With the development of new protocols such as Mimblewimble and zk-Rollup, as well as the involvement of Layer 2 networks, we see a future where privacy can be better preserved without compromising efficiency and security. Balanced regulatory efforts and user education are also essential to creating a secure and trusted blockchain ecosystem. As such, blockchain technology continues to evolve and offer increasingly sophisticated solutions for maintaining privacy in cryptocurrency transactions.

Key Security and Privacy Challenges Facing Cryptovaluta Transactions

One of the main challenges faced by cryptovaluta transactions is the transparency of transactions. The blockchain, which functions as a distributed ledger, allows everyone to see all transactions ever made. This means that anyone can trace the flow of funds from one address to another. While these addresses are pseudonymised, further analysis can reveal the identity of the owner. This openness raises privacy concerns especially for users who value anonymity in their financial transactions (Henckel, 2023) .

Another security challenge is the potential for attacks against blockchain networks, such as the Sybil attack. In these attacks, attackers create multiple fake

identities to gain control of the decentralised network. As such, they can influence consensus decisions or even perform a 51% attack, where they gain the majority of hashing power and can alter transaction history (Giordano, 2021) . This threat shows that even though blockchains have sophisticated security mechanisms, there are still risks that need to be considered, especially in terms of centralising power in mining pools or specific entities (Bruschi et al., 2022) .

Users of cryptovaluta should store their private keys with the utmost care. Loss or theft of private keys means that users lose access to their cryptovaluta assets. Hackers often target individuals and cryptocurrency exchanges with phishing attacks, malware, or exploitation of weaknesses in network security to steal private keys and crypto assets. While security technology is constantly evolving, there are always possible loopholes that can be exploited, emphasising the need for secure storage methods such as hardware wallets (Mattassoglio ., 2021)

Regulatory constraints are also a significant challenge in securing cryptovaluta transactions. On the one hand, regulation is necessary to prevent the use of cryptovaluta in illegal activities such as money laundering and terrorism financing. On the other hand, the application of overly strict rules can reduce the appeal of cryptovaluta, which is often seen as a relatively anonymous means of payment. Moreover, compliance with regulations that vary from country to country also makes it difficult for global cryptovaluta exchanges and users to ensure they stay within the law. There is a delicate balance between providing privacy to users and complying with existing regulations (Gerlings & Constantiou ., 2022)

As blockchain technology evolves, innovative solutions such as the zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) protocol are being introduced to improve transaction privacy. These protocols allow transactions to be verified without revealing sensitive details. In addition, user education is also crucial to ensure that they can properly secure their assets and avoid fraudulent schemes. Well-informed users will be more likely to recognise signs of security threats and take appropriate precautions (Gippini ., 2022)

As such, the cryptocurrency market offers many opportunities but also faces major challenges related to security and privacy. The openness of transactions on the blockchain can potentially reveal the identity of users, and the risk of attacks on the network and digital theft remains. In addition, regulation and legal compliance present additional complexities in the use of cryptovaluta. The development of new technologies and increased user education are important steps to improve the security and privacy of cryptocurrency transactions. With the right approach, these challenges can be managed, enabling the growth of a more secure and trusted cryptocurrency market.

Conclusion

Security and privacy in cryptovaluta transactions through blockchain technology, it was found that although blockchain offers some significant advantages in supporting transparent and immutable transactions, it still faces major challenges in terms of privacy. The inherent transparency characteristic of blockchain can lead to over-disclosure, where information about transactions is publicly visible and potentially reveals the identity of the user. Privacy technologies such as zk-SNARKs and CoinJoin are beginning to be developed to address this issue by offering ways to hide certain transaction details, creating a balance between transparency and privacy.

From a security perspective, while blockchain itself is difficult to hack due to its decentralised nature, its security relies heavily on individual user practices and exchange platform security. Threats such as digital wallet theft, phishing attacks, and vulnerabilities in smart contracts can thwart efforts to keep digital assets safe. Therefore, it is imperative to continue developing more advanced security solutions while strengthening user education on potential risks. The combination of advanced technology and in-depth user knowledge is key to improving security and privacy in the cryptocurrency ecosystem.

References

Aalders, A. (2023). Cultivating Organizational Excellence. *Management for Professionals*, *Query date: 2024-12-25 09:37:59*. https://doi.org/10.1007/978-3-031-26289-0

Agdere, K. (2024). *Analyse van de effectiviteit van de MICA-verordening, een Europees juridisch kader voor cryptocurrencies*. *Query date: 2024-12-25 09:37:59*. https://documentserver.uhasselt.be/bitstream/1942/44028/1/4a46adb1-2963-4c62-8d52-11e8e49e3ca9.pdf

Bruschi, D., Rusconi, D., & Zoia, M. (2022). La diversificazione delle tecnologie blockchain. *Osservatorio Del Diritto Civile e …*, *Query date: 2024-12-25 09:37:59*. https://doi.org/10.4478/106697

Callens, E. (2021). Financial instruments entail liabilities: Ether, bitcoin, and litecoin do not. *Computer Law &Security Review*, *Query date: 2024-12-25 09:37:59*. https://www.sciencedirect.com/science/article/pii/S0267364920300996

Campo, A. (2021). *Blockchain, NFT &Crypto Art Stato dell'arte di una nuova tecnologia, approcci e sviluppi= Blockchain, NFT &Crypto Art State of art of a new technology, approaches …*. webthesis.biblio.polito.it. https://webthesis.biblio.polito.it/20545/

Cornelis, N. (2023). *Blockchain en GDPR*. documentserver.uhasselt.be. https://documentserver.uhasselt.be/handle/1942/40925

Gerlings, J., & Constantiou, I. (2022). Machine Learning in Transaction Monitoring: The Prospect of xAI. *arXiv Preprint arXiv:2210.07648*, *Query date: 2024-12-25 09:37:59*. https://arxiv.org/abs/2210.07648

Giordano, A. (2021). La blockchain per lo sviluppo reale. *Esperienze d'Impresa*, *Query date: 2024-12-25 09:37:59*. https://doi.org/10.57570/104714

Gippini, S. (2022). *Marketing e nuove tecnologie nel settore moda: Perché vengono utilizzate dalle aziende? Query date: 2024-12-25 09:37:59.* https://tesi.supsi.ch/4694/1/Gippini_Sara_Tesi_Bachelor.pdf

Grosemans, A. (2022). *Analyse van de intentie tot het gebruik van cryptocurrency*. *Query date: 2024-12-25 09:37:59.* https://documentserver.uhasselt.be/bitstream/1942/38435/1/0f0daf16-4326-4dd3-8835-57c7e272d040.pdf

Henckel, K. (2023). Issues of conflicting laws-a closer look at the EU's approach to artificial intelligence. *Nederlands Internationaal Privaatrecht*, *Query date: 2024-12-25 09:37:59.* https://research.rug.nl/files/703737216/2023-12.pdf

Iovane, G., & Rapuano, A. (2021). *Analisi dei requisiti per infrastruttura Blockchain in ottica di scalabilità e decentralizzazione*. *Query date: 2024-12-25 09:37:59.* https://www2.enea.it/it/Ricerca_sviluppo/documenti/ricerca-di-sistema-elettrico/adp-mise-enea-2019-2021/tecnologie-per-la-penetrazione-efficiente-del-vettore-elettrico-negli-usi-finali/report-rds_ptr_2020_029.pdf

Lia, F. D., Schioppo, R., Presti, R., Pizzuti, S., Romano, S., & ... (2021). *Implementazione delle logiche di gestione per gli smart building di seconda generazione*. *Query date: 2024-12-25 09:37:59.* https://www2.enea.it/it/Ricerca_sviluppo/documenti/ricerca-di-sistema-elettrico/adp-mise-enea-2019-2021/tecnologie-per-la-penetrazione-efficiente-del-vettore-elettrico-negli-usi-finali/report-rds_ptr_2021_008.pdf

Macchia, L., & Giugno, A. (2022). *Cryptovalute: Inquadramento fiscale del fenomeno e potenziali usi pathologici*. torrossa.com. https://www.torrossa.com/it/resources/an/5445193

Mattassoglio, F. (2021). Le proposte europee in tema di crypto-assets e DLT. Prime prove di regolazione del mondo crypto o tentativo di tokenizzazione del mercato finanziario .... *Rivista Di Diritto Bancario*, *Query date: 2024-12-25 09:37:59.* https://boa.unimib.it/bitstream/10281/317607/1/mattassoglio_Riv.%20diritto%20bancario%202021.pdf

Micheletti, I. (2020). *Art-Tech: Blockchain come opportunità di valorizzazione partecipata*. dspace.unive.it. http://dspace.unive.it/handle/10579/18311

Milan, L. (2022). *Blockchain: La spina delle criptovalute e del web 3.0*. dspace.unive.it. http://dspace.unive.it/handle/10579/22375

Mintas, I. (2023). *De belastingheffing op inkomsten uit cryptocurrencies in het Belgische fiscaal recht*. documentserver.uhasselt.be. https://documentserver.uhasselt.be/handle/1942/40960

Mooij, A. (2023). Currency (Layering). *... to Prevent Money Laundering and the Financing of ...*, *Query date: 2024-12-25 09:37:59.* https://doi.org/10.1007/978-3-031-46417-1_6

Muciaccia, N., & Lopopolo, S. (2022). A First Glance at the Relationship between NFTs and Intellectual Property. *Orizzonti Del Diritto Commerciale*, *Query date: 2024-12-25 09:37:59.* https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/oidldoco2022&ion=46

Sabry, F. (2021). *Gedecentraliseerde Financiën: Het apocalyptische evenement voor de traditionele financiële instellingen*. books.google.com. https://books.google.com/books?hl=en&lr=&id=qJSLEAAAQBAJ&oi=fnd&pg=PT

578&dq=security+privacy+cryptovaluta+transactions+blockchain+technology&ots=J4TBCeyJJJ&sig=3EbcZDEwXWgV_of2s7B2xW345DE
Sanusi, I. (2015). Bridging Qualitative and Quantitative Research. *Journal of Da'wah Science*,*4* (13), 409-409. https://doi.org/10.15575/jid.v4i13.400
Sartori, J. (2020). *Il mobile payment e il suo impatto sull'ecosystema del settore dei pagamenti*. dspace.unive.it. http://dspace.unive.it/handle/10579/18090
Syafril, S., & Erlina, N. (2018). *Preparing Interview Protocols, Selecting Informants and Probing in Qualitative Research*. *Query date: 2024-05-25 20:59:55.* https://doi.org/10.31219/osf.io/pvsh3
Veuger, J. (2020). Blockchain Convergentie ... *Een Nieuwe Economie En Samenleving Met Blockchain*, *Query date: 2024-12-25 09:37:59.* https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/blockchain-convergentie-jan-veuger-2020.pdf
Victor, O. (2021). *An Evolution on How Countries Tax Virtual Currencies: Is There a Consensus Evolving*. search.proquest.com. https://search.proquest.com/openview/da147ba927088bf7ac47fc84a06c16f3/1?pq-origsite=gscholar&cbl=2026366&diss=y
Wekke, I. S. (2020). *Qualitative Research Design*. *Query date: 2024-05-25 20:59:55.* https://doi.org/10.31219/osf.io/4q8pz