THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 4. Issue 1 (2024)
https://doi.org/ 10.62019/abbdm. v4i1.119.

ASIAN BULLETIN OF BIG DATA MANAGEMENT
ISSN (Print): 2959-0795
http://abbdm.com/
ISSN (online): 2959-0809

Enhancing Security and Confidentiality in Decentralized Payment System Based on Blockchain Technology

Seema Sultana Bhurgri, Najma Imtiaz Ali, Imtiaz Ali Korejo, Imtiaz Ali Brohi*

Chronicle

Article history

Received: February 23, 2024
Received in the revised format: March 17, 2024
Accepted: March 20, 2024
Available online: March 21, 2024

Seema Sultana Bhurgri, Najma Imtiaz Ali, Imtiaz Ali Korejo are currently affiliated with the Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan.
Email: seema.bhurgri@gmail.com
Email: najma.channa@usindh.edu.pk
Email: imtiaz@usindh.edu.pk

Imtiaz Ali Brohi is currently affiliated with Government College University Hyderabad, Pakistan.
Email: brohiimtiaz@hotmail.com

***Corresponding Author:**

Abstract

The advent of blockchain technology (BC), has revolutionized the financial landscape with its decentralized, immutable, and verifiable characteristics. Blockchain technology can be deployed in many applications, however the Decentralized Payment System (DPS) can be considered as the most widely used application among all others. The public nature of early decentralized payment systems (e.g. bitcoin) has led to privacy challenges, making them susceptible to cybercriminal activities such as ransomware attacks and illegal financial transactions. This research investigates various decentralized payment systems adopted in blockchain technology and outlines the security requirements necessary to safeguard user transactions. The objectives of this study include examining payment transactions in decentralized systems, identifying potential threats, proposing improved and efficient security solutions, and assessing personal data sharing confidentiality.

Keywords: Blockchain (BC); Decentralized Payment System (DPS); Security; Ransomware attacks.

INTRODUCTION

Payment systems are experiencing significant transformations, primarily driven by technological advancements. These shifts involve a reduced reliance on cash and an increasing emphasis on rapid payment solutions, such as online payment. Online payment enables the transfer of money through the internet, making the process straightforward in the current era. While online payment transactions have become highly popular, some individuals misuse this system to manipulate others' finances. Efforts are underway to explore various solutions to address this issue, although stopping such crimes entirely remains a challenge. Traditionally, cash served as the primary medium of transactions, with people engaging in buying and selling using physical currency. Then, debit and credit cards became popular. You could use these cards to buy things, but both you and the seller had to pay some money to the bank. Sometimes, there were risks like someone trying to take money without permission. So, payment transactions had their challenges. Over the past few years, there has been a substantial shift in the payment landscape. In today's world, paying for things online is pretty simple. Now, there are new ways to pay that are not part of the main blockchain, and these seem like they could be really good. Encouraging the successful output of blockchain systems has been an important research problem. Assessing the overall landscape of payment systems, blockchain has brought about a significant transformation. Decentralized payment system also called cryptocurrencies has emerged as the most prevalent and impactful aspect of the payment system, introducing considerable changes. People increasingly express interest in this system, given its ability to securely store payment transactions. Blockchain is a pretty new trend that has been greatly influenced by the popularity of Bitcoin and its capacity to create a trust network for facilitating financial operations in the world. In the year 2008, Nakamoto (2008) familiarized blockchain technology with the goal of eliminating intermediaries by enabling decentralized transactions. The proposal involved a peer-to-peer distributed record to facilitate direct payments from payers to payees within the blockchain system, utilizing consensus mechanism (Guo et al., 2016). It is with distinguished characteristics like decentralization, immutability and verifiability (Lin et al., 2018) privacy, transparency, redundancy and integrity (Wüst et al., 2018).

The decentralized payment system is probably the most developed blockchain application. Bitcoin, a well-known decentralized payment system does not trust on reliable third parties, and keep track of transactions on a distributed ledger (i.e blockchain) in contrast to traditional e-cash methods e.g., a central bank (Sandar & Ta-Shma 1999; Chaum, 1983). The blockchain is mostly replicated by nodes that distrust one another and is chronologically connected by a hash. Formerly decentralized payment systems, such as Bitcoin (Nakamoto, 2008), Ethereum (Wood, 2014) and Mixcoin (Bonneau et al., 2014) made transaction data, including sender and receiver addresses and transferred value public in order to guarantee the stability of the blockchain ledger. It has corresponding privacy encounters, for instance in the privacy of identity and transferred price. An attacker can analyze transaction records in the blockchain to figure out the connection among users' addresses and even can obtain the user's actual identity (Reid and Harrigan, 2013; Ron and Shamir, 2013).

Paper Sketch

The continuing parts of the paper are well-ordered as follows. The extant literature on decentralized payment systems (DPS) are reviewed, Moreover the problem statement and paper contribution are described respectively, followed by preliminaries. After that the research method and research design of the proposed framework for enhanced security solution for DPS are provided. Finally, conclusion is given.

LITERATURE REVIEW

In conventional payment methods, reliance on trusted third parties is essential. This confidence leads to the creation of circulated payment record data across several organizations, that may be public without the explicit agreement or disagreement of users. Numerous researches have previously suggested decentralized payment schemes (Hatefi et al. 2023; Miao et al. 2022, Ahmed et al. 2021; Kapoor et al. 2021; Rahithya 2021, Lin et al. 2020; Asamoah et al. 2020; Thanapal et al. 2020; Alansari 2020; Fanti et al. 2019; Fauzi et al. 2019; Zhong et al. 2019; Qin et al. 2017; Heilman et al. 2016; Chen et al. 2014). Typically, various schemes have been proposed, including the following: In 2023, Hatefi et al. (2023) presented an electronic payment protocol blockchain-based which used false names to keep the secrecy of real users. Furthermore, secret sharing and fair blind digital signature are used to attain the essential attributes of secure electronic payment systems and confidentiality. In 2021, Kapoor et al. (2021) tried to develop a solid DCAP framework, a Condition Anonymous Payment (CAP) conspire (in light of proposed mark of information), whose security can be exhibited under the characterized formal semantic and security models. In their proposed work there is an effective Advanced Decentralized Contingent Anonymous Payment (DCAP) framework that tries to find some kind of harmony among security assurances and guideline. Proposed Framework tried to achieved both anonymity and guideline properties in decentralized restrictive anonymous payment (DCAP) system. In 2021, Ahmed et al. (2021) focusing on that it is certainly difficult to sort out promising scam transactions by a middle man. Also proposed framework aims at resolving issues regarding security and insignificance, is fully based on blockchain system. An algorithm is proposed that make consumers capable to transact through cryptocurrency using blockchain networks. Completely different from the flat system where consumers can do transaction without any need of third party and vendors can also be comforted with their transaction. This type of transaction will be very easy for both consumers and vendors. During transaction process, the consumers along with the vendor can see the complete transaction, such as date, time and everything that they dealt with when the transaction was held.

In 2021, Rahithya et al. (2021) proposed a Conditional Anonymous Payment (CAP) scheme that is designed to achieved both anonymity and regulation properties to make the solid decentralized conditional anonymous payment (DCAP) system. By posing significance of scheming a decentralized payment system that strikes a stability between attaining reasonable secrecy, protection and permitting regulation. In 2020, Lin et al. (2020) presented solid Decentralized Conditional Anonymous Payment (DCAP) and demonstrated how the related security requirements can be satisfied. As well as regulation it considers the existing value-hiding technologies to further enhance user privacy. Decentralized Anonymous Payment (DAP) system is difficult to regulate. Consequently, the anonymity characteristic of blockchain can be broken by criminals for money laundering and other cybercrime such as ransomware attacks. The DCAP scheme including some trusted nodes for managing the authority of users, it also used smart contracts to retrieve certificates.

In 2019, Fauzi et al. (2019) concentrated to the constraint inherent in certain DAP systems (such as Zerocash and Monero), where the inability to eliminate addresses with unknown balances poses a challenge. In particular, the researchers utilized updatable keys along with efficient zero-knowledge arguments to develop Quisquis. This system not only ensures privacy and anonymity that conceals the specific real amount but also skillfully removes addresses of zero amount. In 2017, Qin et al. (2017) took into account regulatory aspects in formulation of a DAP (Decentralized Autonomous Payment) system. They specifically put forward a tangible system built on blind signatures and a key derivation mechanism. This system successfully attains properties such as transferability, anonymity, and resistance to double-spending. In 2019, Fanti et al. (2019) discussed principles and design of the decentralized payment systems. Such a payment system needs to be decentralized at several layers due to the sensitive nature of money. The system's design and development would be decentralized to ensure that its implementation is free of control from any single party. Blockchain Technology is a pretty new trend and can possibly be used in a wide number of applications. Amongst all these the Decentralized Payment System (DPS) can be said as one of the most efficient and mature blockchain application with widespread adoption. DPS don't have faith on trusted third parties (e.g., a central bank) and uses Blockchain Technology to record the transactions. In early designs of DPS all the transaction data was made public to ensure the consistency of the blockchain (Lin et al. 2018). This has corresponding privacy challenges, such as privacy of real name identity and the amount of money transaction between two parties. The transaction records in the blockchain can be analyzed by an attacker and it can create correlation between users' address and even can find the actual identity of the user (Ron & Shamir 2013). In order to address this issue and to provide solutions to enhance privacy for decentralized payment systems, the mixing technology has been suggested (Sandar &Ta-Shma 1999; Nakamoto 2008; Fauzi et al. 2019), but still with some limitations such as higher computational complexity and lengthier waiting delay.

Some Researchers proposed a number of solutions based on cryptographic tools (Bissias et al., 2014, Ruffing et al., 2014) to strengthen the privacy protection of DPS but later pointed out privacy threats by the attackers. There have also been further researches aiming on the design of secure DPS and few study regulation (that is compulsory to reduce misuse / criminal exploitation) (koshy et al. 2014; Valenta and Rowan 2015; wu et al. 2019). However, the DPS can't be efficiently controlled. However these systems can easily be exploited for criminal activities, such as money laundering and in cybercrime cases (e.g., payment of ransom for ransomware / online extortion cases) (Qin et al., 2017).

"Consequently, the security and privacy challenges are still faced by decentralized payment systems. Due to its public nature, it can be a magnet for online fraud and money laundering and lacks consumer data protection and it is mostly unregulated.

RESEARCH CONTRIBUTION

In response to the identified limitations above; This research aim is to address these challenges by providing a secure, efficient, and privacy-preserving mechanism for decentralized transactions. We introduce a secure and efficient enhanced solution for decentralized payment system (DPS) adopted in blockchain technology (BC) that tries to achieve relevant security requirements necessary to safeguard user transactions. Accordingly;

- **Investigation of Decentralized Payment Transactions:** Analyzing the dynamics of payment transactions within decentralized payment systems, with a focus on blockchain technology.

- **Identification of Threats:** Assessing potential threats associated with data breaches in decentralized payment systems, including vulnerabilities to cyber ransomware attacks.

- **Proposal of Enhanced Security Solutions:** Developing and proposing solutions to enhance the security of decentralized payment systems, addressing identified threats and vulnerabilities outlines the security requirements necessary to safeguard user transactions.

- **Confidentiality and Anonymity Examination:** Evaluating the confidentiality and anonymity of personal data shared in blockchain-based online transactions, aiming to secure against illegal activities such as online extortion and money laundering.

- **Analysis of Proposed Solution:** Comparing the proposed enhanced security solution with other decentralized payment systems to analyze security and privacy flaws, providing insights into its effectiveness.

PRELIMINARIES

Blockchain Technology (BC)

It is a recent, promising and revolutionary technology. Over the last decade it has achieved a lot of attention. It is renovating everything from Payment transactions to almost many areas that are now adopting the BC technology to store and share data among parties without any involvement of the middleman. In Blockchain technology the way of storing information can be done in a different way, in which data is recorded in the form of blocks that are cryptographically connected and structured in consecutive order, so that both privacy and security can be provided simultaneously.

In 2008, Nakamoto (2008) introduced blockchain technology as a means to eliminate intermediaries by facilitating peer-to-peer transactions. The proposal included the utilization of a peer-to-peer distributed ledger to achieve this objective. According to this proposition, individuals making payments can directly transact with recipients through the blockchain network, facilitated by consensus mechanisms (Guo et al., 2016). The blockchain is characterized as a distributed ledger shared among all participating entities, each identified by public keys (IDs) and accessible through their respective private keys. Moreover, the blockchain confirms robust trustworthiness among peers involved in communications (Sharma et al., 2019). Blockchain system offers the different properties like confidentiality, public verifiability, integrity, redundancy, and transparency (Wüst & Gervais, 2018).

KEY FEATURES OF BLOCKCHAIN

Blockchain technology can be defined by its main features that enhance to its distinctive and influential capabilities:

- **Decentralization:** The decentralized nature the blockchain can be said as one of the major features of it. Without depending on a central authority the information is spread through a network of computers called nodes, that makes the system strong and less susceptible to even a single point of failure (Lin et al. 2020).

- **Distributed Ledger:** A distributed ledger is maintained by the blockchain and it records the transactions happening across all contributing nodes. To ensure that all participants having same and recent version/ copy of data, the ledger is updated and synchronized in real time (Sharma et al., 2019)

- **Immutability:** When information is added to the blockchain, it becomes very hard to modify or interfere with. Every block is linked to the previous one by using cryptographic hashes, and then the chain of blocks is created that provides the confidential and unaltered information (Wüst et al., 2018).

- **Transparency:** All the participants that are in a blockchain network can access the same information adopting transparency. And all the transactions are visible to all authorized peers, encouraging reliance and accountability (Wüst et al., 2018).

- **Consensus Mechanisms:** To agree on the validity of transactions blockchain networks use consensus algorithms. Example includes a popular mechanism Proof of Work(PoW) (Li et al. 2021).

- **Security:** Cryptographic techniques are used by blockchain to secure transactions and control access to data. Cryptographic keys such as public and private are used to enhance the user interactions, data integrity and security when transactions take place (Lin et al. 2020).

- **Privacy and Anonymity:** To provide a level of privacy, participants are identified by cryptographic addresses rather than showing their personal information. That makes transactions transparent. Degree of anonymity can be varying on different blockchain platforms (Wüst et al., 2018).

- **Tokenization:** The blockchain network includes the creation and interchange of digital tokens. These tokens can signify various possessions, for example digital assets, cryptocurrencies or even real-world assets, that provides a method for value transfer inside the blockchain ecosystem (Lin et al. 2020).

DECENTRALIZED PAYMENT SYSTEM

A decentralized payment system refers to a financial framework that works independently of an intermediary or a central authority to control or conduct transactions. Unlike traditional payment transaction system that are managed by financial institutions such as banks, decentralized payment system functions without a central entity overseeing and to validate the transactions. In place they employ blockchain technology and cryptographic techniques and principles to enable peer to peer transactions, removing the need for a central entity. Some modules and processes are involved in the working of decentralized payment system that includes:

- ***Blockchain Technology***

A decentralized payment system trust on blockchain technology, an immutable and secure decentralized database that records transactions. This blockchain is sustained by a collective network of computers, working together to process and validate transactions (Miers, 2017).

- ***Decentralization***

Decentralized anonymous payment systems based on the decentralization. The absenteeism of an intermediary or central authority means that transactions and funds are in the control of users those who own assets and have overall control on it. In addition, decentralization makes the system robust to attacks or tries to manipulate transactions (Miers, 2017).

- ***Mining***

To validate a transaction, the mining process is used and add them to the blockchain. Miners practice algorithms and validate communications (Miers, 2017).

- ***Anonymity***

A high degree of anonymity is provided in decentralized payment systems by applying pseudonyms instead of real identities. This creates it challenging for malign agents to track or perceive transactions, that provides a top level of confidentiality and safety (Chen et al. 2014).

RESEARCH METHODOLOGY

Our research focuses to make transactions more secure and to overcome these privacy flaws that are related to users' real identity, payment details and address that are targeted by the cybercriminals to breach the sensitive data and information.

This research intends to adopt an experimental computer science research method.

- Real World Problem will be addressed.
- Solution is proposed on an existing DPS.
- Evaluation of given solution by using quantifiable and non-quantifiable data.
- Comparison of our proposed improved and enhanced security solution for DPS with other existing Decentralized Payment Systems frameworks.
- Analysis of Privacy and security flaws in existing and new proposed research for DPS.
- Final Results

Our research aims to employ an experimental computer science research method to address a real-world problem associated to decentralized payment systems (DPS). The main attention lies on developing a framework that propose an improved and enhanced solution to efficiently tackle the addressed challenges. The proposed solution will go through a rigorous process during evaluation, using both quantifiable and non-quantifiable data. This multi-layered assessment aims to provide a broad understanding of the proposed solution's performance and usefulness in addressing the real-world problem at hand.

A comparative analysis is conducted to contextualize the proposed enhanced solution within the comprehensive landscape. It includes measuring our DPS improved solution against other present decentralized payment systems, assisting us to differentiate its strengths, flaws, and distinctive features. A critical facet of our research contains a detailed analysis of confidentiality and security features inherent in both the existing DPS frameworks and our newly proposed enhanced solution. This analysis pursues to identify and address any potential weaknesses and exposures, confirming the strength and reliability of the proposed work.

The conclusive phase of our research produces final results that combine the findings from the evaluation, comparison, and security analysis. These findings not only provide valuable vision to the area of decentralized payment systems but also lead for more enhancement and optimization, highlighting a guarantee to addressing real-world challenges with advanced and effective solutions.

CONCLUSION

The growing nature of this study, coupled with the worldwide importance of decentralized payment system like cryptocurrencies, explains the investigation of innovative ways for researchers. This research adopts a computer science research method employing a present decentralized payment transaction system with improved privacy feature. The proposed system aims to mitigate the risks related with cybercriminal decision and ransomware attacks grounded on decentralized payment systems, contributing to the generally security and privacy background of blockchain technology.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Ahamed, S., Siddika, M., Islam, S., Anika, S., Anjum, A., & Biswas, M. (2021). BPS: Blockchain Based Decentralized Secure and Versatile Light Payment System. *Asian Journal of Research in Computer Science*, *May*, 12–20. https://doi.org/10.9734/ajrcos/2021/v8i430206

Alansari, S. (2020). *A blockchain-based approach for secure, transparent and accountable personal data sharing* (Doctoral dissertation, University of Southampton).

Asamoah, K. O., Xia, H., Amofa, S., Amankona, O. I., Luo, K., Xia, Q., ... & Guizani, M. (2020). Zero-chain: A blockchain-based identity for digital city operating system. *IEEE Internet of Things Journal*, *7*(10), 10336-10346.

Bissias, G., Ozisik, A. P., Levine, B. N., & Liberatore, M. (2014, November). Sybil-resistant mixing for bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (pp. 149-158).

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. (2014). Mixcoin: Anonymity for bitcoin with accountable mixes. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18* (pp. 486-504). Springer Berlin Heidelberg.

Chaum, D. (1983, August). Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto 82* (pp. 199-203). Boston, MA: Springer US.

Chen, X., Li, J., Ma, J., Lou, W., & Wong, D. S. (2014). New and efficient conditional e-payment systems with transferability. *Future Generation Computer Systems*, *37*, 252-258.

Fanti, G., & Viswanath, P. (2019). *Decentralized Payment Systems: Principles and Design*. https://dtr.org/wp-content/uploads/2019/01/2019-01-16-Decentralized-Payment-Systems-Principles-and-Design.pdf

Fauzi, P., Meiklejohn, S., Mercer, R., & Orlandi, C. (2019). Quisquis: A new design for anonymous cryptocurrencies. In *Advances in Cryptology–ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings, Part I 25* (pp. 649-678). Springer International Publishing.

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial innovation*, 2, 1-12.

Hatefi, Z., Bayat, M., Alaghband, M. R., Hamian, N., & Pournaghi, S. M. (2023). A conditional privacy-preserving fair electronic payment scheme based on blockchain without trusted third party. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 10089–10102. https://doi.org/10.1007/s12652-021-03672-1

Heilman, E., Baldimtsi, F., & Goldberg, S. (2016, February). Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions. In *International conference on financial cryptography and data security* (pp. 43-60). Berlin, Heidelberg: Springer Berlin Heidelberg.

Kapoor, C., Vishnuvardhan, R., Shivadeepak, V., & Charan, M. S. (2021). *An advanced Decentralized Conditional Anonymous Payment System for Cryptocurrency using Blockchain*. *8*(5).

Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in bitcoin using p2p network traffic. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18* (pp. 469-485). Springer Berlin Heidelberg.

Li W, Feng C, Zhang L, Xu H, Cao B, Imran MA (2021) A Scalable Multi-Layer PBFT Consensus for Blockchain. In: IEEE Trans- actions on Parallel and Distributed Systems, pp. 1146-1160,

Lin, C., He, D., Huang, X., Choo, K. K. R., & Vasilakos, A. V. (2018). BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of network and computer applications*, *116*, 42-52.

Lin, C., He, D., Huang, X., Khan, M. K., & Choo, K. K. R. (2020). DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain. *IEEE Transactions on Information Forensics and Security*, *15*, 2440–2452. https://doi.org/10.1109/TIFS.2020.2969565

Miao, J., & Han, Z. (2022, February). An decentralized anonymous payment confidential transactions with efficient proofs and scalability. In *2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)* (pp. 1347-1351). IEEE.

Miers, I. (2017). *Decentralized Anonymous Payments*. https://www.semanticscholar.org/paper/fec1ef1fddfbe97cff5fececd375dbd294bbe418

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Qin, B., Chen, L. C., Wu, Q. H., Zhang, Y., Zhong, L., & Zheng, H. B. (2017). Bitcoin and digital fiat currency. *Journal of Cryptologic Research*, *4*(2), 176-186.

Rahithya, S. E., & Reddy, D. L. N. (2021). *ISSN NO : 0377-9254 VERSATILE LIGHT PAYMENT SYSTEM USING SECURE AND EFFICIENT DECENTRALIZED CONDITIONAL ANONYMOUS PAYMENT Page No : 424 Vol 12 , Issue 12 , DEC / 2021 ISSN NO : 0377-9254 Page No : 425*. *12*(12), 424–429.

Reid, F., & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197-223). Springer New York.

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17* (pp. 6-24). Springer Berlin Heidelberg.

Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014). Coinshuffle: Practical decentralized coin mixing for bitcoin. In *Computer Security-ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II 19* (pp. 345-364). Springer International Publishing.

Sander, T., & Ta-Shma, A. (1999). Auditable, anonymous electronic cash. In *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19* (pp. 555-572). Springer Berlin Heidelberg.

Sharma, V., You, I., Jayakody, D. N. K., Reina, D. G., & Choo, K. K. R. (2019). Neural-blockchain-based ultrareliable caching for edge-enabled UAV networks. *IEEE Transactions on Industrial Informatics*, *15*(10), 5723-5736.

Thanapal, K., Mehta, D., Mudaliar, K., & Shaikh, B. (2020). Online Payment Using Blockchain. *ITM Web of Conferences*, *32*, 03007. https://doi.org/10.1051/itmconf/20203203007

Valenta, L., & Rowan, B. (2015). Blindcoin: Blinded, accountable mixes for bitcoin. In *Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers* (pp. 112-126). Springer Berlin Heidelberg.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

Wu, Y., Fan, H., Wang, X., & Zou, G. (2019). A regulated digital currency. *Science China Information Sciences*, *62*, 1-12.

Wüst, K., & Gervais, A. (2018, June). Do you need a blockchain?. In *2018 crypto valley conference on blockchain technology (CVCBT)* (pp. 45-54). IEEE.

Zhong, L., Wu, Q., Xie, J., Li, J., & Qin, B. (2019). A secure versatile light payment system based on blockchain. *Future Generation Computer Systems*, 93, 327-337.