[11]Layth Almahadeen
[2]Renzon Daniel Cosme Pecho
[3]Murugananth Gopal Raj
[4]Nichenametla Rajesh
[5]Zainab Mohammed Imneef
[6]Sayali Karmode Yelpale

Digital Investigation Forensic Model with P2P Timestamp Blockchain for Monitoring and Analysis

Journal of Electrical Systems

Abstract: - Forensic analysis of Blockchain data is a new field in police work. It's now one of the largest problems facing law enforcement. The paper discussed the worldwide need for digital forensics in law enforcement and Blockchain forensics to counteract crimes committed using Blockchain technology. It's been said that we've entered a new age of technology that's heavily dependent on the principles of Blockchain. The research produced a set of guidelines for Digital Investigators. on addition, a theoretical framework grounded on the concept of regular activity has been developed, and a legislative framework has been proposed to ensure that its illegal purpose will always be punished severely.

Keywords: Blockchain Technology; Digital Forensic Investigators; Blockchain Forensics.

I. INTRODUCTION

The study of applying forensic methods to the investigation of blockchain technology and the data it generates is known as "blockchain forensics," and it is a fast expanding topic. The technology behind Bitcoin and other cryptocurrencies is blockchain, a distributed ledger that keeps records of transactions in a way that is both safe and transparent. The necessity for forensic investigation of this data has grown in significance with the widespread use of blockchain technology.

Blockchain forensics has several uses, one of which is the investigation of financial crimes including money laundering and terrorism funding. Because blockchain data is public and cannot be altered, it may be used to track the origin of money and spot fraudulent behavior.The use of digital evidence in forensic investigations is projected to grow as a means of connecting individuals with criminal acts [1-3].

Blockchain is the distributed and unchangeable record that powers cryptocurrencies like Bitcoin and Ethereum. It keeps a complete and transparent record of all financial transactions made across an electronic network of computers. Blocks of transactions are cryptographically linked together to create a chain, thus the term "blockchain." Blockchain's security and openness make it a desirable technology for use in areas outside cryptocurrency trading.[4-6]

The Need for Blockchain Forensics

While blockchain technology offers several advantages, its pseudonymous and decentralized nature also presents unique challenges. Criminals and malicious actors have exploited these characteristics to engage in activities like money laundering, ransomware attacks, and the sale of illegal goods and services on the dark web. Traditional financial institutions and law enforcement agencies have struggled to adapt to these new challenges, necessitating the development of specialized techniques and tools for blockchainforensics[7-10].

The Role of Blockchain Forensics

[1]Lecturer, Department of Financial and Administrative Sciences, Al- Balqa' Applied University, Jordan, Email: layth.mahadeen@bau.edu.jo, ORCID: 0000-0002-6680-2781
[2]Professor, Department of Biochemistry, Universidad San Ignacio de Loyola, Lima, Peru, Email: rcosme@usil.edu.pe
[3]Professor and Head, Department of Electrical and Electronics Engineering, Ahalia School of Engineering and Technology, Kerala, India, Email: gmurugananth@gmail.com
[4]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Andhra Pradesh, India, Email: nrajeshcse@kluniversity.in
[5]Lecturer, Department of Dentistry, Al-Zahrawi University College, Karbala, Iraq, Email: nomansudad@gmail.com
[6]Assistant Professor, Department of Information Technology, MGM College of Engineering, Maharashtra, India, Email: sayalis.karmode@gmail.com

Blockchain forensics involves the investigation of blockchain transactions to uncover illicit activities and provide critical insights for law enforcement, regulators, businesses, and individuals. Key aspects of blockchain forensics include:

Transaction Analysis: Experts use blockchain analysis tools to examine transaction details, including sender and receiver addresses, transaction amounts, and timestamps. This analysis helps in identifying suspicious or fraudulent activities[11].

Address Clustering: Blockchain forensics experts employ advanced techniques to cluster multiple addresses belonging to the same entity. This is critical for tracking the flow of funds and understanding the behavior of actors on the blockchain[12].

Anomaly Detection: Deviations from typical blockchain transaction patterns can signal potential fraud or cybercrime. Forensic analysts use anomaly detection algorithms to flag suspicious activities for further investigation[13].

Cryptocurrency Tumbling and Mixing Analysis: Criminals often attempt to obfuscate the source of their funds by using tumbling or mixing services. Blockchain forensics can help trace the origin of mixed or tumbled cryptocurrencies[14].

Regulatory Compliance: Businesses operating in the cryptocurrency space are subject to regulatory requirements. Blockchain forensics aids in ensuring compliance with anti-money laundering (AML) and Know Your Customer (KYC) regulations[15].

Evidence for Legal Proceedings: Blockchain forensics findings are often used as evidence in legal cases related to cryptocurrency crimes, fraud, or disputes[16].

Risk Assessment: Individuals and businesses can use blockchain forensics services to assess the risk associated with specific cryptocurrency transactions or addresses.

The need for blockchain forensics

The need for blockchain forensics arises from several critical factors and challenges associated with blockchain technology, particularly in the context of cryptocurrencies. Here are some of the key reasons why blockchain forensics is essential:

Illicit Activities and Criminal Use:Cryptocurrencies, like Bitcoin, have been used for various illicit activities, including money laundering, drug trafficking, tax evasion, and cybercrime[17].

Criminals often leverage the pseudonymous nature of blockchain transactions to hide their identities and the origins of funds[18].

Fraud Prevention and Detection:In the world of Initial Coin Offerings (ICOs) and token sales, fraud is a significant concern. Blockchain forensics can help verify the legitimacy of projects and identify fraudulent schemes.

Financial Regulation and Compliance:Regulatory authorities around the world are increasingly recognizing cryptocurrencies as financial assets. This requires businesses operating in the crypto space to adhere to anti-money laundering (AML) and Know Your Customer (KYC) regulations.Blockchain forensics tools help businesses comply with these regulations by monitoring and analyzing transactions for suspicious activity[19].

Asset Recovery and Investigations:In cases of cryptocurrency theft or fraud, blockchain forensics can aid law enforcement agencies in tracking and recovering stolen assets[20].It provides crucial evidence for legal proceedings, making it possible to identify culprits and hold them accountable.

Security and Trust:Asblockchain technology becomes integral to various industries (e.g., supply chain, healthcare, finance), ensuring its security and trustworthiness is paramount.[21]Blockchain forensics helps in identifying vulnerabilities, potential threats, and suspicious activities that could compromise the integrity of blockchain networks.

Risk Mitigation for Investors and Businesses:Investors in cryptocurrencies and blockchain-based projects need to assess the risk associated with their investments.Businesses dealing with cryptocurrencies or blockchain technology need to conduct due diligence to avoid engaging with fraudulent or high-risk entities.

Protection Against Insider Threats:In organizations using blockchain technology for record-keeping or supply chain management, insider threats can be a concern.Blockchain forensics can help detect and prevent unauthorized or fraudulent actions by employees or other insiders.

Transaction Transparency and Accountability:Blockchain forensics enhances the transparency and accountability of blockchain networks. It ensures that transactions are recorded accurately and that participants can be held accountable for their actions.

Regulatory Oversight:Governments and regulatory bodies are increasingly recognizing the need to oversee and regulate the cryptocurrency space.Blockchain forensics data can be used by regulators to assess the compliance of crypto businesses with existing financial laws.

II. LITERATURE SURVEY

IoT forensics was initially suggested in 2013 by EdewedeOriwoh et al. [15]. As the first model of its kind in the field of IoT forensics, the proposal to use a 1-2-3 area technique to DF research pertaining to the IoT has been made. In 2015, after years of refinement, Shams Zawoad initially defined IoTF [16]. Expand DF to include IoT, investigate the DF procedure for IoT gadgets, and provide a precise description of IoTF. Ana Nieto et al. have done ground-breaking work to address the privacy concerns around Internet of Things forensics. In 2016, Ana Nieto et al. published a lengthy article on "digital witnesses" [17], the first journal article on forensics research on the Internet of Things. This article proposed the concept of "digital witness" and gave its formal definition, discussed the new concept in personal devices, and further defined the basic components for realizing this concept in future work. The EDFIM (improved digital forensic investigation model) was examined by Ana Nieto and colleagues in 2017. A privacy-aware IoT forensics model (PROFIT) [19] is suggested to include the privacy protection standards of the 1974 "US Privacy Act" and ISO/IEC 29100:2011 [18] across the whole investigation life cycle. From the vantage point of IoT security, 2017's literature [20] highlighted the major problems in IoT forensics. This article first introduces the Internet of Things (IoT) and its fundamental components before moving on to explore the IoT's three-tier architecture and the primary challenges surrounding IoT forensics. The lack of standardization and the diversity of IoT devices are factors discussed in the literature [21]. Forensics in smart homes, wearable devices, and smart cities are used to illustrate a suggested digital forensic investigation model (DFIM) tailored to these and other IoT application situations. In an IoT-specific DF investigation, the DFIM model may be used to gather, examine, evaluate, and report on sufficient forensic evidence. In order to address issues like the unstandardization of IoT devices and the dearth of connection, the literature [22] suggested the notion of forensic state acquisition controller (FSAC). In addition, it suggests a broad framework and a technique for determining the forensic state of IoT devices. The first journal literature review on Internet of Things forensics [23] was released in 2018 by Maxim Chernyshev and colleagues. The author provides a short history of digital forensics model development in the IoT context before moving on to explore the outstanding issues that arise when trying to apply these models to Internet of Things gadgets. In order to discover illegal facts based on IoT systems, the literature [24] presents a forensic investigation architecture that makes use of public digital ledgers. It does this by securing the evidence of interactions between diverse IoT things in public, distributed, and decentralized blockchain networks. Data identification and categorization techniques gleaned from the Internet of Things are discussed in the literature [25] as a means of unearthing the most compelling evidence at crime scenes. Tools and methods are provided for discovering and tracking IoT devices. The term "digital footprint" is relatively new to the world of criminal justice and is based on a mapping of the frequency and interactions between devices. A blockchain-based IoT Forensics Framework (BIFF) was developed in the literature [26] to address IoT security concerns; BIFF keeps track of the history of digital evidence in a way that protects users' anonymity while maintaining transparency and accountability. The literature [27] explored the complexities of forensics in the IoE age, including the analysis of the real digital forensics process and the obstacles that occur, as well as the challenges of the IoT forensics standards. From the standpoint of cloud forensics, which is concerned primarily with resolving security problems generated by client data after consumers quit using cloud services, the aforementioned literature [28] investigates emerging security vulnerabilities. After deleting or pausing customer data utilizing cloud services, it may be reconstructed using a suggested framework. An analysis of the digital

footprints of Internet of Things (IoT) devices was published in 2019 [29] by Francesco Servida et al., who believe that the exponential growth of IoT devices has not been matched by an equivalent improvement in digital forensics tools and procedures, leading to security and privacy concerns. With the goal of putting IoT to use in the smart home industry, the prospects and obstacles of IoT forensics are examined. Fog computing forensics, monitoring, and troubleshooting will all rely heavily on historical network traffic archives, as discussed in [30] of the cited literature. In addition, we offer a novel system architecture for building a trusted, encrypted, but queryable network traffic file for fog-assisted IoT applications, which seamlessly integrates searchable encryption with trustworthy hardware. A forensic analysis model was developed in the literature [31], which can gather and analyze data from a wide range of IoT devices to aid in investigations. Making use of recovered forensic evidence Cases with Clear Digital Evidence for Forensics Intelligent Retail Cloud Smart Home Internet Investigative System Incriminating Evidence Forensic Evidence Forensic Evidence Analysis Report of Forensic Harvest Testing The Internet of Things Forensics IoV Generalized Model. Network Safety and Data Transfer The author illustrates how to use the suggested paradigm to guide the forensic examination of IoT devices using the widely used Amazon Echo as an example. An automated knowledge-sharing forensics platform is proposed [32] in the literature, with the ability to automatically recommend a forensic mode based on case data. The leading international publication IEEE Internet of Things publication published a review of forensics on the Internet of Things by JianweiHou et al. in 2020 [33]. The leading international publication IEEE Communications Surveys & Tutorials [34] published a review of Internet of Things forensics by Stoyanova et al. ,e appearance of these two leading journal review papers indicates that IoTF is gaining increasing attention in the academic community. They provide a systematic review of IoTF's development over the past decade and summarize the classic forensic models and forensic methods. They also provide a detailed discussion of the key issues that have been resolved and remain unresolved in the forensics process, including the applicability of technology and legal boundary issues, and data security and privacy concerns.

Concept of Blockchain Technology

The blockchain idea transformed the standard trading mechanism into an immutable digital record, making it more technically sophisticated and reliable across the board. Blockchain is short for a global distributed ledger that keeps track of each and every digital asset transaction, both permanent and temporary. Every record is stored in a block to improve openness, accountability, tracking, portability, and confidence in the data. The creation process is represented by this sequence of blocks [9]. There are three main ideas central to blockchain theory: a. P2P architecture, where information is shared and recorded between users. b. It logs the time and date of each communication. c. Rules-based and secure consensus procedures.

Peer-to-Peer (P2P)

Nodes in a blockchain-based system create a network of interconnected computers. Members of nodes construct and operate this network, which is hosted on the internet. The function and location of each node in this network is a defining characteristic. These hubs serve as identifiers for the network classification. The following diagram depicts the differences between a decentralized network and a centralized network. The interconnected computers in a peer-to-peer network function as if they were equals. P2P is a distributed network design because of this feature. The jobs have been divided up fairly amongst the nodes. No need to send information via a centralized server for sharing data between nodes, as seen in Figures 1 and 2.

Figure 1: Centralised Server Network.

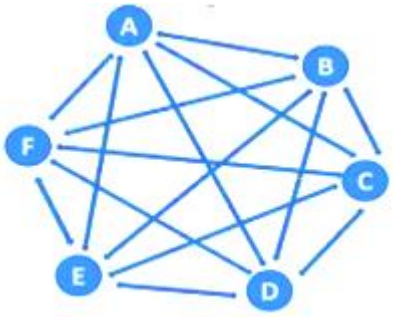

Figure 2: Peer to Peer Network.

Store Messages in Timestamp

Addition of messages, data, or files to the blocks guarantees the veracity and openness of the data among the nodes by including a timestamp.

Consensus Mechanisms with Rules and Security

The consensus mechanisms model of the blockchain emphasizes the fact that all network members agree on a state of decision. The consensus algorithm provides a mechanism for maintaining data synchronization among the many nodes that make up a network. When it comes to reaching a worldwide consensus on a network update, the value of each method is different. That means it's adaptable for everyone. This vulnerability is due to the fact that nodes may be customized. Proof of Work, Proof of State, Delegated Proof of Stake, Proof of Importance, Proof of Capability, Proof of Activity, Proof of Authority, Proof of Burn, etc. are just a few examples of the many different kinds of consensus techniques that may be used.

Assessing the Loopholes Respond to Unsolved Crimes

The paradigm of technology is evolving into a more sophisticated form. When it comes to protecting sensitive consumer data, blockchain technology is one of the most cutting-edge options available. However, it has been stated that the number of cybercrimes committed on blockchain platforms, such as money laundering and the use of non-fungible tokens (NFTs), is progressively growing. The Federal Bureau of Investigation (FBI) has just formed a new division inside the organization called the National Cryptocurrency Enforcement Team (NCET). The task force's mission is to stop criminals from misusing blockchain and other cryptocurrencies. The NCET will keep an eye on the confiscation of digital assets and illegal use of blockchain technology. Digital forensics and blockchain forensics are the focus of this section [10]. The development of specialized, cutting-edge cyber units is indicative of the gravity of the problem. To confront increasingly sophisticated criminal activity, many nations' forensic laboratories and police forces lack the necessary digital infrastructure. Blockchain-based crimes provide a novel challenge for law enforcement in most developing nations. There aren't even effective rules in place to deal with these kinds of offenses. Many blockchain-related matters have not yet been resolved since they call for sophisticated resources and personnel. analyzed what must be done to solve the case and get the convictions.

Digital Forensic Investigation Model

When investigating crimes, a digital forensic model may be a useful tool for law enforcement. In accordance with the model, we need to make sure that this has been looked at by a forensics professional. We may potentially construct two stages where it applies. One is the use of blockchain technology in event tracking via the implementation of the smart contract idea, and another is the potential role that technological countermeasures may play [16]. The digital forensic investigation model is shown in the following diagram. This elucidates the areas of concern for a digital forensics investigator. An investigator's viewpoint should center on the characteristics of the smart contract itself. In the online world, you may find a plethora of Ponzi schemes that promise you instantaneous returns of 100%, 300%, or even 10,000% on whatever money you put toward the purchase of bitcoin. Since there was previously no oversight for exchanging money earned over the Internet, the cryptocurrency industry has been booming. However, things have changed, and governments now tax cryptocurrency transactions. This area had a higher risk for Ponzi schemes. With the advent of the smart contract idea, the blockchain may now be modified to steal from investors. The same is true for the data chain. These smart

contracts are inscribed digitally on digital assets; a profitable scheme is promoted; investors put money into it without verifying its legitimacy. The model predicts a false occurrence, so individuals put money into it and then file a false complaint. The model has made it quite evident that dangers are there. Here, a digital investigator is responsible for handling these procedures and removing the technological obstacle associated with raising public knowledge about the need for them to refrain from engaging in such behavior. Whatever worries there were, one of the standard operating procedures has dealt with them. If a digital investigator wants to trace a chain back to its beginning, they need to focus on the technical details. Therefore, the investigative process may be strengthened and enhanced by using blockchain technology and smart contracts. (See

.Fig. 3)

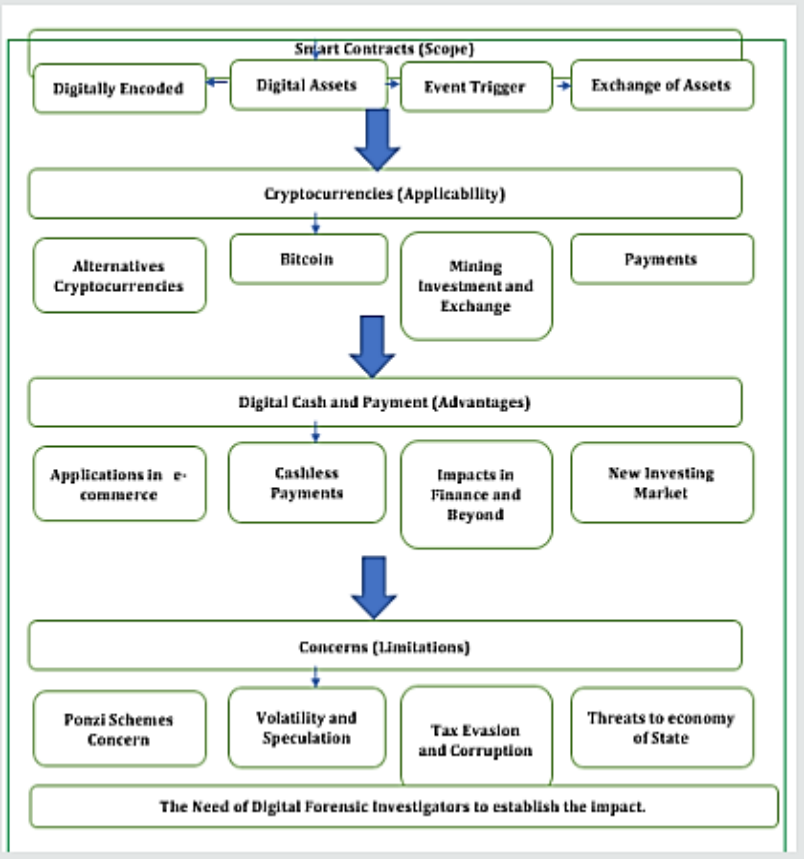

Figure 3: Digital Investigation Forensic Model.

Five T model

Numerous pieces of writing and research confirm blockchain technology's veracity and incorruptibility. However, it has been noted that the true function of a blockchain-based technology or money is kept secret. The paradigm of digital inquiry provides conclusive evidence of this. This paper proposes the five 'T' model of transparency, traceability, tracking, transferability, and trust to guarantee the efficacy of digital forensic approaches. The regulations of digital forensic investigators suggest that these five Ts be guaranteed in every use of blockchain technology throughout the world [17].

Transparency

The digital forensics investigator's approach to the crime scene must be open and comprehensible to the court. All smart contract requirements must be taken seriously and made public for any blockchain-based product or event. Blockchain events' true nature and intent must be decoded by the corresponding smart contract.

Traceability

A blockchain custody system must be developed for the data stored there. With this information, the criminal's digital footprints may be traced back to him. Blockchain is a data format that enables the creation of a distributed, time-stamped ledger. If a crime can be tracked, it's much simpler to find the perpetrator.

Tracking

Experts in digital forensics can do a forensic audit of bitcoin transactions. The law requires constantly basing its findings on factual investigation. Expert opinion suggests that wallet-to-wallet data tracking is possible.

Transferability

Several permission-less blockchains exist, allowing us to guarantee that the transfer of data will be carried out under the watchful eye of digital forensic investigators or a monitor. The ability to transfer ownership guarantees transactions are tracked and recorded.

Trust

The existing literature indicated that blockchain technology was an option accompanied by a great deal of trust concerns and misunderstanding. Model for conducting effective digital forensics investigations has been developed.

Preventive Measures

This study proposes a theoretical framework for preventing fraud in blockchain technology, with its foundations in the model and theory of everyday activity. The awareness factors before using the blockchain technology are covered by the repercussions of regular activity theory and the safety procedures.

Real-world examples of Blockchain forensics in action

Blockchain forensics has been used in various real-world cases to investigate and address illicit activities, fraud, and regulatory compliance. Here are some notable examples of blockchain forensics in action:

Silk Road Investigation (2013):The Silk Road was an infamous online marketplace for illegal drugs and other illicit goods, operating on the dark web.Law enforcement agencies, including the FBI, used blockchain forensics to trace Bitcoin transactions associated with the Silk Road. The analysis of blockchain data played a crucial role in identifying and arresting the site's operator, Ross Ulbricht, and confiscating a significant amount of Bitcoin as evidence.

Mt. Gox Hack (2014): Mt. Gox, once the largest Bitcoin exchange, suffered a major hack that resulted in the loss of hundreds of thousands of Bitcoins. Blockchain forensics experts helped track the movement of stolen Bitcoins through the blockchain. This analysis contributed to the recovery of some stolen funds and provided valuable information for legal proceedings.

Ransomware Investigations: Ransomware attacks involve criminals encrypting victims' data and demanding crypto currency payments for decryption keys.Blockchain forensics has been used to trace ransom payments and identify the wallets controlled by cybercriminals.

In some cases, authorities have been able to freeze or seize these assets, disrupting ransomware operations.

ICO Scam Investigations: Initial Coin Offerings (ICOs) have been associated with numerous scams and fraudulent projects.Blockchain forensics experts have helped investors and regulators identify fraudulent ICOs by analysing blockchain transactions, identifying token movements, and exposing deceptive practices.

Crypto Exchange Investigations: Crypto currency exchanges have faced various challenges, including security breaches and regulatory compliance.Blockchain forensics tools assist exchanges in monitoring transactions for suspicious activity, ensuring compliance with AML and KYC regulations, and identifying security vulnerabilities.

Dark Web Marketplaces: Blockchain forensics has been used to track transactions on dark web marketplaces where illegal goods and services are bought and sold.Law enforcement agencies have identified and arrested individuals involved in illegal activities by tracing cryptocurrency transactions.

Regulatory Compliance: Crypto currency businesses and financial institutions use blockchain forensics to meet regulatory requirements. This includes verifying the source of funds, conducting AML checks, and ensuring compliance with KYC regulations.

Supply Chain Management: In supply chain applications of blockchain, forensics can be used to trace the origin of products and verify the authenticity of goods.It helps prevent counterfeit products and ensures transparency in supply chains.

Token Fraud in DeFi (Decentralized Finance): DeFi platforms have seen instances of token fraud and rug pulls (exit scams).Blockchain forensics tools are used to analyze smart contract interactions and token movements to detect suspicious behavior and protect investors.

These examples illustrate the diverse range of applications for blockchain forensics, from law enforcement investigations to fraud prevention and compliance monitoring. As blockchain technology continues to evolve, so too will the methods and tools used in the field of blockchain forensics to address emerging challenges and threats.

III. CONCLUSION

Blockchain forensics monitoring and analysis are essential tools in the fight against cryptocurrency-related crime and the responsible adoption of blockchain technology. As crypto currencies and decentralized applications continue to evolve, so too will the methods and techniques used in blockchain forensics. This field will remain a critical component of the broader blockchain ecosystem, helping to strike a balance between innovation and security in the digital world.

REFERENCES

[1] X. Xu, Q. Huang, H. Zhu et al., “Secure service offloading for internet of Vehicles in SDN-enabled mobile edge computing,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3720–3729, 2021.

[2] X. Liang and Y. Kim, “A Survey on Security Attacks and Solutions in the IoT Network,” in Proceedings of the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference, (CCWC), pp. 0853–0859, NV, USA, June 2021.

[3] W. Zhou, “Reviewing IoT security via logic bugs in IoT platforms and systems,” IEEE Internet of 1ings Journal, vol. 8, 2021.

[4] N. Miloslavskaya and A. Tolstoy, “Internet of ,ings: information security challenges and solutions,” Cluster Computing, vol. 22, no. 1, pp. 103–119, 2019.

[5] E. Al-Masri, Y. Bai, and J. Li, “A Fog-Based Digital Forensics Investigation Framework for IoT Systems,” in Proceedings of the 2018 IEEE International Conference on Smart Cloud (SmartCloud), pp. 196–201, New York, NY, USA, September 2018.

[6] V. R. Silvarajoo, S. Yun Lim, and P. Daud, “Digital evidence case management tool for collaborative digital forensics investigation,” in Proceedings of the 2021 Digital Evidence Case Management Tool for Collaborative Digital Forensics Investigation, pp. 1–4, CRC, Langkawi Island, Malaysia, January 2021.

[7] M. Elhoseny, M. M. Selim, and K. Shankar, “Optimal deep learning based convolution neural network for digitaforensics face sketch synthesis in internet of things (IoT),” International Journal of Machine Learning and Cybernetics, vol. 12, no. 11, pp. 3249–3260, 2020.

[8] Z. Su, H. Wang, H. Wang, and X. Shi, “A Financial Data Security Sharing Solution Based on Blockchain Technology and Proxy Re-encryption Technology,” in Proceedings of the 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), pp. 462–465, Chongqing City, China, November 2020.

[9] D. Sathya, S. Nithyaroopa, D. Jagadeesan, and I. J. Jacob, “Block-chain technology for food supply chains,” in Proceedings of the 2021 1ird International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 212–219, Tirunelveli, India, February 2021.

[10] K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, “A proxy Re-encryption approach to secure data sharing in the internet of things based on blockchain,” IEEE Systems Journal, vol. 16, no. 1, pp. 1685–1696, 2022.

[11] G. Kumar, R. Saha, C. Lal, and M. Conti, “Internet-of-Forensic (IoF): a blockchain based digital forensics framework for IoT applications,” Future Generation Computer Systems, vol. 120, no. 120, pp. 13–25, 2021.

[12] M. Li, C. Lal, M. Conti, and D. Hu, “LEChain: a blockchainbased lawful evidence management scheme for digital forensics,” Future Generation Computer Systems, vol. 115, no. 6, pp. 406–420, 2021.

[13] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, vol. 107, pp. 841–853, 2020.
[14] G. Liang, J. Xin, Q. Wang, X. Ni, and X. Guo, “A BlockchainBased Internet of ,ings Forensics Model,” in Advances in Artificial Intelligence and Security, pp. 687–696, Springer, New York, NY, USA, 2021.
[15] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, “Internet of things forensics: challenges and approaches,” in Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 608–615, Austin, TX, USA, June 2013.
[16] S. Zawoad and R. Hasan, “FAIoT: towards building a forensics aware eco system for the internet of things,” in Proceedings of the 2015 IEEE International Conference on Services Computing, pp. 279–284, New York City, NY, USA, June 2015.
[17] A. Nieto, R. Roman, and J. Lopez, “Digital witness: safeguarding digital evidence by using secure architectures in personal devices,” IEEE Network, vol. 30, no. 6, pp. 34–41, 2016.
[18] Iso, “Information technology - Security techniques - Privacy framework,” 2020, https://www.iso.org/standard/73722.html.
[19] A. Nieto, R. Rios, and J. Lopez, “A methodology for privacyawareIoT-forensics,” in Proceedings of the 16th IEEE International Conference on Trust, Security And Privacy in Computing and Communications, pp. 626–633, Sydney, NSW, Australia, October, 2017.
[20] M. Banday, “Enhancing the security of IOT in forensics,” in Proceedings of the International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, India, October 2017.
[21] T. Zia, P. Liu, and W. Han, “Application-specific digital forensics investigative model in internet of things (IoT),” in Proceedings of the 12th International Conference on Availability, Reliability and Security, New York; NY, USA, September 2017.
[22] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, “Forensic state acquisition from internet of things (FSAIoT),” in Proceedings of the 12th International Conference on Availability, Reliability and Security, ACM ,Calabria, Italy, August 2017.
[23] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, “Internet of things forensics: the need, process models, and open issues,” IT Professional, vol. 20, no. 3, pp. 40–49, 2018.
[24] M. Hossain, R. Hasan, and S. Zawoad, “Probe-IoT: a public digital ledger based forensic investigation framework for IoT,” in Proceedings of the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, Paris, France, June 2018.
[25] F. Bouchaud, G. Grimaud, and T. Vantroys, “IoTforensic,” in Proceedings of the 13th International Conference on Availability, Reliability and Security, IEEE, Hamburg, Germany, August 2018.
[26] D. P. Le, H. Meng, L. Su, S. L. Yeo, and V. ,ing, “BIFF: a blockchain-based IoT forensics framework with identity privacy,” in Proceedings of the TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, Korea, October 2018.
[27] A. Macdermott, T. Baker, and Q. Shi, “Iot forensics: challenges for the ioa era,” in Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, Paris- France, February, 2018.
[28] J. Surbiryala and C. Rong, “Secure customer data over cloud forensic reconstruction,” in Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, January 2018.
[29] F. Servida and E. Casey, “IoT forensic challenges and opportunities for digital traces,” Digital Investigation, vol. 28, pp. S22–S29, 2019.
[30] H. Duan, Y. Zheng, C. Wang, and X. Yuan, “Treasure collection on foggy islands: building secure network archives for internet of things,” IEEE Internet of 1ings Journal, vol. 6, no. 2, pp. 2637–2650, 2019.
[31] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, “IoT forensics: Amazon Echo as a use case,” IEEE Internet of 1ings Journal, vol. 6, no. 4, pp. 6487–6497, 2019.
[32] X. Zhang, K. K. R. Choo, and N. L. Beebe, “How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform,” IEEE Internet of 1ings Journal, vol. 6, no. 4, pp. 6850–6861, 2019.
[33] J. Hou, Y. Li, J. Yu, and W. Shi, “A survey on digital forensics in internet of things,” IEEE Internet of 1ings Journal, vol. 7, no. 1, pp. 1–15, 2020.
[34] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A Survey on the Internet of ,ings (IoT) Forensics: Challenges, Approaches and Open Issues,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020.