Forensic Science International: Digital Investigation 42 (2022) 301470

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models

Alex Akinbi [a, *], Áine MacDermott [a], Aras M. Ismael [b]

[a] School of Computer Science and Mathematics, Liverpool John Moores University, 3 Byrom Street, Liverpool, L3 3AF, United Kingdom
[b] Information Technology Department, College of Informatics, Sulaimani Polytechnic University, Sulaymaniyah, Iraq

ARTICLE INFO

Article history:
Received 15 February 2022
Received in revised form
13 September 2022
Accepted 15 September 2022
Available online xxx

Keywords:
Blockchain
IoT forensics
Digital forensics
IoT

ABSTRACT

Digital forensic examiners and stakeholders face increasing challenges during the investigation of Internet of Things (IoT) environments due to the heterogeneous nature of the IoT infrastructure. These challenges include guaranteeing the integrity of forensic evidence collected and stored during the investigation process. Similarly, they also encounter challenges in ensuring the transparency of the investigation process which includes the chain-of-custody and evidence chain. In recent years, some blockchain-based secure evidence models have been proposed especially for IoT forensic investigations. These proof-of-concept models apply the inherent properties of blockchain to secure the evidence chain of custody, maintain privacy, integrity, provenance, traceability, and verification of evidence collected and stored during the investigation process. Although there have been few prototypes to demonstrate the practical implementation of some of these proposed models, there is a lack of descriptive review of these blockchain-based IoT forensic models.

In this paper, we report a comprehensive Systematic Literature Review (SLR) of the latest blockchain-based IoT forensic investigation process models. Particularly, we systematically review how blockchain is being used to securely improve the forensic investigation process and discuss the efficiency of these proposed models. Finally, the paper highlights challenges, open issues, and future research directions of blockchain technology in the field of IoT forensic investigations.

1. Introduction

Internet of Things (IoT) forensics is described as a branch of digital forensics, where the identification, collection, organization, and presentation processes deal with the IoT infrastructures to establish the facts about a criminal incident (Zawoad and Hasan, 2015). The proliferation of IoT devices used in smart homes, commercial environments, medical facilities, and the energy sector has led to a paradigm shift and growing interest in IoT forensic research. In recent times, we have also witnessed the vast development of software applications, gadgets, and virtual assistants that enable remote monitoring and management of several IoT devices, especially in smart homes (Akinbi and Berry, 2020). By the end of 2018, there were an estimated 22 billion IoT-connected devices in use around the world and forecasts suggest there will be around 50 billion IoT devices in use around the world by 2030 (Statista, 2020). Forensic investigators, law enforcement agents, and legal experts have also taken a significant interest in IoT forensics due to the proliferation of these devices (Chung et al., 2017). The always active, always generating characteristic of these devices makes them excellent digital witnesses, capturing traces of activities of potential use in investigations (Servida and Casey, 2019). Digital evidence from IoT devices has also been used in several criminal cases (BBC, 2018; Hauser, 2017). The inherent vulnerabilities of these devices have also made them susceptible to threats by cybercriminals who continue to launch highly disruptive and large-scale attacks with increasing levels of sophistication (Chernyshev et al., 2018). Hence, making IoT forensics is crucial to digital investigations and incident response for the foreseeable future.

However, the fast pace of development and nature of IoT environments brings a variety of forensics challenges which include evidence identification, collection, preservation, analysis, and correlation (Conti et al., 2018). Forensic examiners have struggled to overcome the existing challenges of IoT forensics especially due to the nature of complex IoT ecosystems and the lack of a standardized

* Corresponding author.
E-mail addresses: o.a.akinbi@ljmu.ac.uk (A. Akinbi), a.m.macdermott@ljmu.ac.uk (MacDermott), aras.masood@spu.edu.iq (A.M. Ismael).

https://doi.org/10.1016/j.fsidi.2022.301470

IoT forensic investigation process. Many of the IoT forensic challenges are well documented in previous studies (Li et al., 2019a; MacDermott et al., 2018; Zhang et al., 2019). Moreover, existing digital forensic tools and methods do not support newer IoT devices. These digital forensic tools are plagued by numerous limitations and are incapable of fitting with the infrastructure of the IoT environment, which is heterogeneous by nature (Ahmed Alenezi et al., 2019; Dawson and Akinbi, 2021). Several IoT forensic models and frameworks have been proposed to address these challenges and help accomplish a thorough investigation, especially in smart home environments. However, their implementation is limited to specific scenarios, scope, and devices. The diversity of IoT devices running proprietary software, limitation of device storage, lack of access to evidential data stored on cloud environments, and variety of native communication protocols used by these devices (Bluetooth Low Energy, Bluetooth, ZigBee, Wi-Fi, NFC, RFID, etc.), makes several IoT forensic investigation process models inadequate for digital evidence admissibility in criminal proceedings.

These existing IoT forensic investigation models also face new challenges including inaccessibility of data from different sources, privacy concerns, privacy laws, data provenances in multiple locations, evidence transparency and traceability, data analysis of large volumes of datasets, etc (Li et al., 2019b). Most notably are the difficulties which surround the secure chain of custody due to increasing data volatility and complex data transit routes among the IoT architecture (Chernyshev et al., 2018; Hegarty et al., 2014). Since IoT forensic evidence data may be gathered from multiple remote locations, which significantly complicates the mission of maintaining a proper chain of custody (O'Shaughnessy and Keane, 2013; Stoyanova et al., 2020). Hence, current research towards new IoT forensic investigation process models has been proposed to address these challenges which adopt the use of blockchain technology. The popularity of blockchain technology and its application has seen a rapid increase in many sections such as finance, smart contracts, logistics, pharmaceutical industries, and cybersecurity (Taylor et al., 2020). Most importantly in the context of this paper, its application to IoT forensics.

The use of blockchain could enable forensics examiners to address issues surrounding evidence traceability, transparency, auditability, and accountability due to the secure and immutable nature of cryptographic hash links between blocks and transactions (Li et al., 2019b). This allows a secure digital chain of custody among trusted IoT devices and architecture. Therefore, creating a guaranteed transparent method of decentralized preservation of digital evidence mitigates the risk that evidence held by a central arbitrator may be accidently corrupted by examiners or damaged by malicious insiders. It is important to identify the existing research specifically related to the application of blockchain technology to the challenges of IoT forensics, to address how several IoT investigation process models offer solutions to address them. To identify what research and forensic models have been proposed for blockchain and IoT forensics, it is necessary to map out relevant research papers and scholarly works systematically.

This paper seeks to focus on existing literature concerning the use of blockchain as a supporting technology for IoT forensic investigation process models, which includes areas of digital forensics related to evidence authenticity, transparency, traceability, integrity, and accountability of forensic evidence and chain of custody within a case examination. The main purpose of this study is to critically examine existing literature and works on blockchain-based forensic investigation process models and use our understanding to develop future research directions.

The rest of this paper is organised as follows. Discussion of related works is presented in Section 2. Section 3 provides a brief overview of the research goals, main contributions and research questions. In Section 4, we discuss and present the research methodology with which the primary studies were selected for the systematic literature review and analysis. Section 5 presents the results and summary of key findings from the selected primary studies. In Section 6, we discuss the results of the related research questions. Section 7 describes open issues and potential future research directions. Finally, Section 8 concludes the paper.

2. Related works

To the best of our knowledge, there are no studies specifically related to Systematic Literature Reviews (SLRs) of blockchain application to IoT forensic investigation models and frameworks. However, there are recent studies that have conducted surveys and SLRs on the application of blockchain to IoT security (Casino et al., 2019; Conoscenti et al., 2016; Salman et al., 2019; Taylor et al., 2020; Yli-Huumo et al., 2016) and IoT forensics in general (Ahmed Alenezi et al., 2019; Atlam et al., 2020; Chernyshev et al., 2018; Hou et al., 2020; Kebande et al., 2020; Kebande and Ray, 2016; Lutta et al., 2021; Stoyanova et al., 2020; Yaqoob et al., 2019). These studies provide a valuable reference point to our study and form the basis for understanding how blockchain technology has been implemented in the IoT research domain. Especially in the field of IoT forensic investigation process models, we discuss and examine in this section topics by selected authors that have influenced our study.

In 2018, Chernyshev and colleagues (Chernyshev et al., 2018) conducted a concise review of the state of the art of conceptual digital forensic models that can be applied to the IoT environment. They concluded that the current conceptual IoT forensic process models still require extensive scientific validations in practice and do not address the confidentiality and integrity of evidence, especially for IoT environments. They recommend reliable process models will be essential to conduct successful digital forensics investigations in IoT environments.

Alenezi et al. (A. Alenezi et al., 2019) conducted a review of the state of the art on IoT forensics in 2019. In the study, they identified and explored several proposed IoT forensic frameworks most notably the Digital Forensic Investigation Framework for IoT (DFIF-IoT) (Kebande and Ray, 2016) which adheres to the ISO/IEC 27043:2015 standard, a Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures (CFIBD-IoT) (Kebande et al., 2017) and a Forensic Investigation Framework for IoT Using a Public Digital Ledger (FIF-IoT) (Hossain et al., 2018b) amongst others. Although the proposed FIF-IoT framework implements a public ledger using blockchain technology to ensure integrity, confidentiality, anonymity, and non-repudiation of the digital evidence, the review is not comprehensive and is limited to the discussion of only this framework.

Atlam et al. (2020) conducted a review of state-of-the-art research and recent studies on IoT forensics investigation process models. Interestingly, they highlighted the lack of suitable forensic tools that can prevent accidental modifications in IoT environment endpoints and the need for a novel IoT forensic investigation process method to address these issues. Moreover, they did not review the application of blockchain to IoT forensics. The study indicated how the use of Artificial Intelligence (AI) can help address some of the challenges and issues associated with various stages of digital forensics investigation lifecycle such as evidence collection, evidence preservation, analysis, and presentation of the evidence.

Similarly, a SLR on the state of IoT forensics was conducted by Hou et al. (2020). They found that 8 out of 58 of the research papers proposed forensic investigation models for IoT. They highlighted that although these models are in the early stages and developed

based on hypothetical case studies, they still face the challenge of maintaining the forensic soundness of digital evidence, especially for IoT forensics which is a prerequisite for admission in a court of law. However, they discussed two models namely Probe-IoT (Hossain et al., 2018a) and FIF-IoT(Hossain et al., 2018b) which use blockchain technology to acquire and preserve evidence in IoT-based systems. Since 2018, the application of blockchain has diversified especially in the field of IoT forensics so our study aims to investigate what research studies currently exist specifically regarding IoT forensic investigation process models and blockchain technology implementation.

Stoyanova et al. (2020) and Lutta et al. (2021)surveyed recent IoT forensics challenges, approaches, and open issues. They highlighted the challenges of maintaining IoT forensic evidence chain of custody. In the study, they presented a brief overview of a few blockchain-based IoT investigation frameworks that have been proposed to secure evidence integrity using decentralized blockchain-based solutions. Their study provides a valuable start to our study since the field of digital forensics and IoT forensics advances quickly. Therefore, it is essential to consider the most recent research approaches and studies specifically for both theoretical and practical blockchain-based IoT forensics models and frameworks as a guide to new research activities in the field of IoT forensics.

3. Research goals and contributions

The purpose of this study is to analyse existing studies, their findings and to summarize the research efforts in the application of blockchain technology to the IoT forensic investigation process. This study focuses on IoT investigation models and frameworks that implement blockchain technology to secure the evidence chain of custody and maintain privacy, integrity, and preservation of forensic evidence collected. To achieve this aim, we developed three research questions that this study attempts to address as presented in Table 1.

This study complements existing research studies by using an SLR to identify primary studies related to blockchain-based IoT forensic investigation models and frameworks up to late 2021. It also provides an up-to-date study and the current state of IoT forensic investigation processes to ensure the integrity of evidence collection, preservation, and secure chain of custody. The study provides IoT forensic researchers and investigators interested in the implementation of blockchain technology in IoT forensics, with a comprehensive review of studies, and presents data to express ideas and considerations in the realm of blockchain-based IoT forensic investigation. Finally, this work provides an opportunity for future research works to investigate and address the open issues and challenges to help ensure a secure and reliable blockchain-based IoT forensic investigation process.

4. Systematic literature review methodology

To achieve the objectives of reviewing the most relevant studies and answering the research questions, we conducted the SLR under the guidance published by Kitchenham and Charters. According to Kitchenham and Charters (2007), a Systematic Literature Review (SLR) is "*a form of secondary study that uses a well-defined methodology to identify, analyse and interpret all available evidence related to a specific research question in a way that is unbiased and repeatable*" (Kitchenham, B. and Charters, 2007).

4.1. Search strings and databases

There are numerous publications on blockchain technology and its application to the IoT forensic investigation process over the years; it is for this reason that we utilised specific keywords and a time frame to search the digital libraries specified to obtain the primary studies. These criteria are necessary to get the most relevant and up-to-date resources for this research. The online digital libraries consulted include IEEE Xplore, Science Direct, ACM Digital Library and Springer Link. These digital libraries are appropriate to conduct the searches as they cover the most relevant topics and credible papers in digital forensic science and software engineering. The libraries were also consulted for simplicity and ease of use. Therefore, the following search strings and keywords were implemented for initiating the search on each of the online libraries:

("blockchain" OR "distributed ledger") AND ("IoT forensics" OR "Internet of Things forensics")

These search strings or keywords above were entered into IEEE Xplore digital library search bar, as well as the Science Direct, ACM Digital Library and the Springer Link (with the Boolean operators AND/OR used as filters for the searches). Primary studies were performed by conducting searches using the online digital libraries on 27th December 2021, to obtain up-to-date academic sources relevant to this study and we considered publications from 1st January 2018 up to 27th December 2021; to produce the primary studies for the Systematic Literature Review.

4.2. Search inclusion and exclusion criteria

It was observed that some of the literature returned from the search results were irrelevant and outside the scope of this study. Therefore, as part of the SLR guidelines, the method of inclusion and exclusion criteria was used to eliminate the irrelevant papers. The criteria for inclusion were based on the selected paper's relevance to blockchain technology and its application to IoT Forensics and IoT Investigation Processes, which must be peer-reviewed and written in English. The exclusion criteria, on the other hand, were

Table 1
Research questions.

Research Questions (RQ)	Discussion
RQ1. What are the latest blockchain-based IoT forensic investigation process models?	There have been notable use cases of blockchain technology in areas such as cryptocurrency, IoT security and cybersecurity in general. Moving beyond these, this research will identify and review two categories of IoT forensic investigation process models based on pubic and permissioned blockchain platforms (see Section 6.1).
RQ2. How is blockchain being used to improve the IoT forensic investigation process?	Practical implementation of blockchain has been deployed in ensuring the integrity of recordkeeping, data privacy and security. This will provide an understanding of blockchain technology used to guarantee the integrity, provenance, privacy, and chain of custody of evidential artefacts collected and stored during IoT forensic investigations (see Section 6.2).
RQ3. How efficient are the blockchain-based IoT forensic investigation process models?	A summary of performance metrics results of selected primary studies with respect to their performance evaluation comparison criteria is presented (see Section 6.3).

based on papers that are not relevant to blockchain technology and its application to IoT Forensics and IoT Investigation Processes. Other exclusion criteria include duplication of published sources, papers not peer-reviewed and literature that is not published in English. The key criteria for inclusion or exclusion of studies are summarized in Table 2.

4.3. Selection of results

The different databases were searched, and the total results from the initial searches carried out using the search strings and keywords on all four online digital libraries generated 6,086 publications. To further refine the results, further checks using the inclusion and exclusion criteria were applied for a more stringent result. With this process, 3,984 publications were excluded from the initial search results, bringing the number down to 2,102 publications. Following that, the exclusion criteria based on titles and abstract was implemented; and as a result, 2,070 publications were also excluded altogether, bringing the number down to 32 primary studies. The 32 publications were read in full, after which a further re-application of the inclusion and exclusion criteria, resulted in the removal of 13 publications. This process brought the total number of primary studies down to 19 papers.

Further implementation of forward and backward snowballing (Achimugu et al., 2014; Wohlin, 2014) to search through citations and references were applied and we identified an additional 4 papers to include. As a result, the total figure for the number of papers to be included is 23.

Finally, the exclusion exercise to refine the results was based on a quality assessment check which focuses on the selected papers' context, date of publication, and relevance to the research questions RQ1, RQ2 and RQ3. Hence, the final set of primary studies for the SLR is 16. Fig. 1 shows the number of publications selected at each stage of the primary studies selection process.

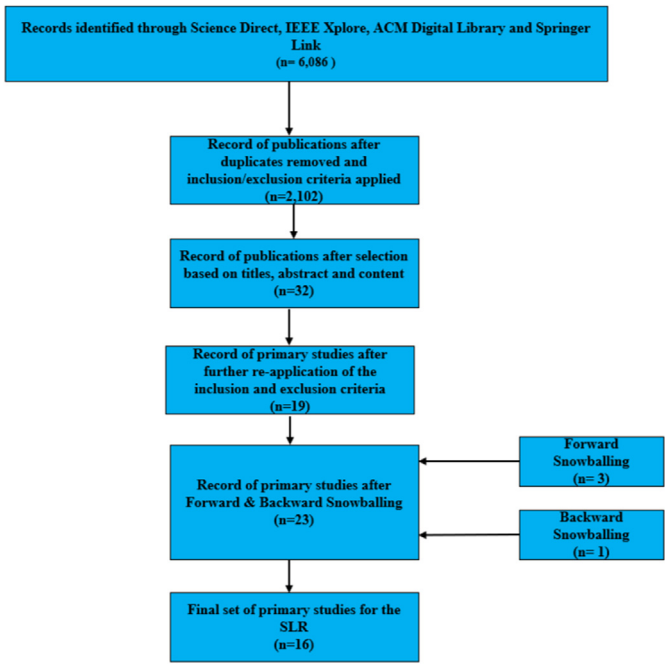

Fig. 1. Selection of primary studies for the SLR.

5. Results

These papers were read in full, and the data extraction process was carried out on them as summarized in Table 3. The 16 papers were classified based on the specific aim of addressing the challenges of securing the evidence chain of custody and maintaining privacy, integrity, and preservation of IoT forensic evidence collected. The themes identified by the studies showed an extensive level of blockchain-based IoT forensic frameworks and models are focused on securing the evidence chain of custody.

Fig. 2 shows the percentages of themes and different applications of blockchain technology to specific areas of the IoT forensic investigation process based on the frameworks and models proposed in our final set of primary studies. The themes identified in the primary studies show that most of the studies use blockchain to maintain the secure *Chain of Custody* (32%). *Data Integrity* is the second most popular theme which accounts for 29%. The proposed frameworks use blockchain to ensure secure, immutable, traceable, and verifiable evidential data collected and stored during IoT forensic investigations. *Data Provenance* is the third most popular theme accounting for 24%, while frameworks that address *Privacy* and *Identity Anonymity* of stakeholders or participants are 15%. These findings also show any framework designed to ensure the integrity of evidential data and secure chain of custody must also compensate for the origin of data accessed by multiple stakeholders involved with the forensic investigation process (from evidence collection, analysis, examination, and presentation). Although most of the primary studies are designed specifically for IoT forensic investigations, few frameworks appear to be generic and can be applied to digital investigations processes including IoT, computer and mobile forensic investigations.

The use of Ethereum blockchain decentralized technology appears to be the most popular blockchain technology used by the majority of the proposed frameworks from the primary studies. This is followed by the use of custom distributed ledgers and Hyperledger blockchain, respectively. Other papers from the pool of

Table 2
Summary of inclusion and exclusion criteria.

Inclusion Criteria	Exclusion Criteria
1. The selected paper must be relevant to blockchain technology application to IoT forensics and IoT forensic investigation process.	1. The paper focuses on the application of blockchain to IoT security.
2. The paper must also provide a practical or theoretical application of blockchain to the IoT forensic investigation process.	2. The paper falls outside the broader field of blockchain technology application to IoT forensics and IoT forensic investigation process.
3. The paper must be peer-reviewed.	3. Papers that are not peer-reviewed.
4. The paper must be written in English language.	4. Papers not written in English and duplicates of published papers.
5. The paper must be published in a conference proceeding or journal	5. Grey literature (white papers, editorial comments, book reviews, government documents and blog posts)

Table 3
Key findings of primary studies.

Primary Study (PS)	Qualitative Data	Blockchain Technology (Consensus Algorithms and/or Blockchain Platforms)	Blockchain Category	Application to IoT forensic investigation
[PS1]	A proof-of-concept blockchain-based IoT forensic chain framework (IoTFC). The framework provides full data provenance, privacy, availability, transparency, traceability, trust, and continuous integrity of IoT forensic artefacts and evidential data.	Custom distributed ledger	Public	Chain of Custody
[PS2]	Blockchain-based IoT forensics framework (BIFF) enhances the integrity, authenticity, and non-repudiation properties for IoT forensic artefacts and evidential data. The proposed framework also provides anonymity for the digital witness/evidence submitter from the public.	Custom distributed ledger & Practical Byzantine Fault Tolerance (PBFT)	Permissioned	Chain of Custody & Privacy and Identity Anonymity
[PS3]	Blockchain-based framework for securely collecting, preserving, and verifying the integrity of digital evidence recovered from compromised IoT networks.	Distributed Hyperledger Fabric	Permissioned	Chain of Custody
[PS4]	This paper focuses on a proof-of-concept multi-blockchain framework that utilizes a cost-efficient approach for guaranteeing integrity and validating provenance. The framework utilizes a combination of low-cost blockchain networks to temporarily store forensic evidence data before permanent storage in an Ethereum blockchain network.	Proof of Stake (PoS) & Multi-chain blockchain	Public	Data Provenance & Data Integrity
[PS5]	This study proposes a proof-of-concept IoT forensic investigation framework (Probe-IoT). The framework is designed to implement the use of a public digital ledger to ensure the integrity, confidentiality, and non-repudiation of digital forensic evidence collected during incident response. The proposed framework is designed to store interactions between IoT devices and their users and store such evidence securely in a distributed blockchain network.	Custom distributed digital ledger	Public	Chain of Custody, Data Provenance & Integrity
[PS6]	Like the IoT forensic investigation framework (Probe-IoT), this blockchain-based forensic investigation framework for IoT (FIF-IoT) provides a mechanism to collect digital IoT forensic artefacts stored in the public digital ledger and verify the integrity of the stored evidence.	Proof of Work (PoW) & Ethereum	Public	Chain of Custody, Data Provenance, Data Integrity & Privacy and Identity Anonymity
[PS7]	A generic and scalable blockchain-based framework (Block-DEF) designed primarily for the scalability, integrity, validity, privacy, and traceability of digital evidence collected and stored in a trusted cloud storage system.	Custom mixed/multi-chain blockchain based on Practical Byzantine Fault Tolerance (PBFT)	Permissioned	Data Provenance, Chain of Custody, Data Integrity & Privacy and Identity Anonymity
[PS8]	A proposed blockchain-based framework that stores all communications of IoT devices in a blockchain. By leveraging the use of Bitcoin or Ethereum, the integrity and transparency of the data can be maintained for forensic investigation purposes.	Proof of Work (PoW) & Ethereum (Geth)	Permissioned	Chain of Custody & Data Integrity
[PS9]	Data provenance and integrity blockchain-based forensic framework (TrustIoV), designed for the Internet of Vehicles (IoV). The proposed system leverages blockchain technology to secure the provenance of digital evidence collected from IoV things.	Custom distributed ledger	Public	Chain of Custody, Data Provenance & Data Integrity
[PS10]	Proposed permissioned blockchain-based framework (Block4Forensic), that provides integrity and provenance of data and evidence collected from smart and connected vehicles for post-accident forensic investigation and analyses.	Custom private digital ledger based on Practical Byzantine Fault Tolerance (PBFT) or Stellar Consensus Protocol (SCP)	Permissioned	Data Provenance, Data Integrity & Privacy and Identity Anonymity
[PS11]	Proof of concept generic blockchain-based framework that provides a data provenance system collects from IoT devices and stores the data in a tamper-proof distributed ledger by leveraging Ethereum.	Ethereum	Public	Data Provenance & Data Integrity
[PS12]	Proposal for the use of a permissioned blockchain-based framework that offers a secure digital evidence storage system that guarantees digital evidence integrity and admissibility.	Raft, Istanbul Byzantine Fault Tolerance (IBFT) & Ethereum (Geth)	Permissioned	Chain of Custody & Data Integrity
[PS13]	A generic proof of concept permissioned blockchain-based framework that enforces integrity, transparency, authenticity, security, and auditability of digital evidence chain of custody.	Hyperledger Composer/Fabric	Permissioned	Data Provenance, Chain of Custody & Data Integrity
[PS14]	The blockchain-based architecture leverages the use of a blockchain consortium to generate and verify the integrity of digital evidence.	Proof of Work (PoW) & Ethereum	Permissioned	Data Provenance, Chain of Custody & Data Integrity
[PS15]	A proof-of-concept blockchain-based framework (LEChain) that leverages Ethereum to manage secure access control, privacy, transparency, and integrity of the entire chain of evidence in digital forensic investigations.	Clique-Proof of Activity (PoA) & Ethereum	Permissioned	Data Provenance, Chain of Custody, Privacy, Data Integrity & Privacy and Identity Anonymity
[PS16]	A proof-of-concept blockchain-based framework, Internet-of-Forensic (IoF) leverages a private multi-blockchain approach on different layers of the IoT architecture and environment for a secure evidence chain of custody.	Hyperledger Fabric & Ethereum (Geth)	Permissioned	Chain of Custody & Privacy and Identity Anonymity

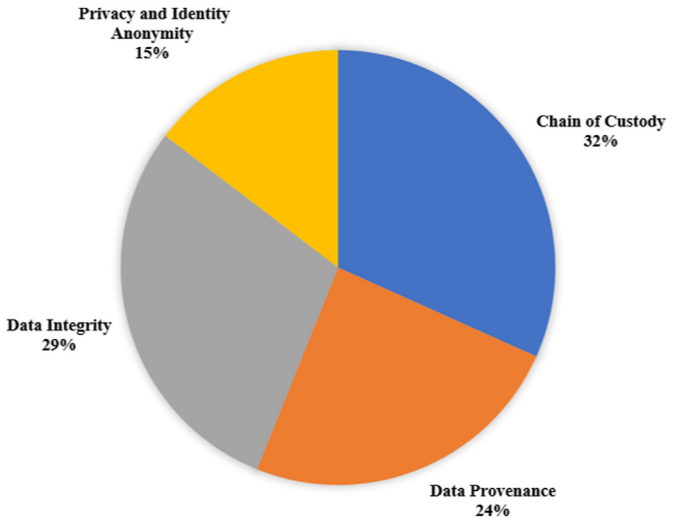

Fig. 2. Blockchain application in IoT forensic investigation process.

primary studies were mostly proposing the use of Merkle signatures for addressing the integrity and data provenance of digital evidence stored and can be accessed securely during the forensic chain of custody. In general, all the primary studies reveal the pivotal role of blockchain technology in addressing the challenges of maintaining the integrity, confidentiality, verification, and non-repudiation of the digital evidence collected and stored during the IoT forensic investigation process.

6. Discussion of results

The application of blockchain since its inception more than ten years ago has gone far beyond its use in finance and cryptocurrencies such as Bitcoin and is currently being applied to solve many practical problems. The preliminary keyword search yielded numerous results on blockchain which shows there is significant and growing interest in the research and application of blockchain technology to provide practical solutions in many areas such as cloud security (Li et al., 2018; Zhu et al., 2019) and IoT security (Khan and Salah, 2018). The majority of the proposed blockchain-based IoT frameworks from the primary studies offer a proof-of-concept application of blockchain in maintaining the integrity, provenance, and secure chain of custody of evidential IoT forensic data.

Notable exceptions that provide practical implementation include judicial use case frameworks for secure electronic evidence chain of custody [PS14] and LEChain [PS15]. Both studies demonstrated the practical application of blockchain by building prototypes based on the Ethereum platform to conduct their experimental analysis. The proof-of-concept blockchain-based investigation frameworks for the Internet of Things [PS8], [PS11] and [P16] which are based on the Ethereum platform, also provided practical implementation using prototypes [PS6] described the use of a custom distributed public digital ledger but used Ethereum for the proof-of-concept experiments. Primary studies [PS7], and [PS9], use custom digital ledgers for their prototypes. In [PS4], the researchers used a hybrid multi-chain proof-of-work mechanism adopting Stellar and EOS to store evidence data blocks in a central database before writing the calculated hash to the Ethereum platform. Forensic-Chain [PS13] is the only proof-of-work that provided implementation built on an Hyperledger Composer prototype.

Overall, the solutions proposed in each framework did not change the existing IoT forensic investigation process but leverage the properties of blockchain technology to ensure the evidence collected and stored during the investigation process is tamper-resistant, immutable, and secure. However, the selection of blockchain technology and platform used depends on factors such as privacy, performance, computational cost, energy consumption, practical implementation, and overall efficiency.

6.1. RQ1. What are the latest blockchain-based IoT forensic investigation process models?

A public or permissionless blockchain is the most in-depth distributed blockchain system and an untainted decentralized mechanism (Chen et al., 2020). It is considered to be transparent because it is open to all users and nodes. However, the drawbacks of the public blockchain are that since the system is open to all nodes and users, it lacks complete privacy and anonymity. This can lead to a weaker network, security of the evidence chain of custody and traceability of the stakeholders' identity. Therefore, the admissibility of digital evidence can be subjected to scrutiny when presented in court. Moreover, anyone can run a node and join the network (Bano et al., 2019). For these reasons, many of the proposed frameworks in the primary studies opted for a permissioned or private blockchain-based investigation model which is restricted to a consortium where all of the identities of all nodes that run the consensus are known, and only authorized access is permitted. Permissioned blockchain is also considered to be more scalable, faster, and energy-efficient compared to the public blockchain. Given these, the latest blockchain-based IoT forensic investigation process models and frameworks are categorized into public and permissioned ones.

- *Public blockchain-based* — Primary studies [PS1], [PS4], [PS5], [PS9], use a mixture of hybridized blockchain which consists of custom public distributed digital ledgers. This is due to their lightweight nature, less resource-intensive processes and networking to hash blocks of transactions compared to well-established platforms like Ethereum adopted by primary studies [PS6], [PS11]. These lightweight blockchain mechanisms are more suitable for heterogeneous IoT environments considering the number of nodes that may be required to process hash blocks and achieve network consensus for public blockchains.
- *Permissioned blockchain-based* — Primary studies [PS2], [PS3], [PS7],[PS8], [P10], [PS12], [PS13], and [PS14], all leverage a permissioned blockchain for the blockchain-based IoT forensic investigation process model where the identity and roles of the authorized forensic investigation stakeholders are known to the other stakeholders. It is also managed in a controlled environment governed by a consortium that deploys it. However, primary studies [PS2], [PS7], [P10], [PS15], and [PS16], are the only permissioned-based blockchain models that implement privacy-anonymity mechanisms to address the issue associated with the identity of all authorized stakeholders.

6.2. RQ2. How is blockchain being used to improve the IoT forensic investigation process?

Considering the heterogeneous nature of IoT, the dimensions of potential evidence collection and the scope of investigations continues to be more challenging. IoT forensic investigations need to identify, preserve, analyse, and present the digital evidence collected from the IoT components in a forensically sound and secure manner. From the primary studies, it is clear that the utilisation of blockchain technologies did not alter the existing IoT forensic investigation process but rather leverages the properties of blockchain for a secure digital investigation process. The inherent

properties of blockchain technology make it resistant to data modification due to its public ledger and consensus mechanisms. Based on the applications of blockchain technology to the IoT forensic investigation process presented from the results of the SLR and the categories identified in RQ1, we discuss how these blockchain-based IoT investigation process models are applied to improve secure evidence chain of custody, maintain privacy, integrity, data provenance and preservation of forensic evidence collected and stored. The latest studies in the SLR suggested the following application of blockchain as follows:

- *Chain-of-custody*— existing digital forensics processes use hash functions to maintain the integrity and prevent modification of evidential artefacts, files and disk images collected and stored during digital forensic investigations. If the hash values for the original and copy are the same, it is highly unlikely that the original and copy are not the same. However, the use of hash functions only validates their integrity but not the examination of events in real-time by forensic stakeholders or custodians, especially for IoT forensics. There is also the probability of hash collisions as most digital extraction tools use either MD5 (Message Digest) or SHA (Secure Hash Algorithm) hashing to check the integrity of digital evidence. This collision can deny the usage of such digital evidence in a court of law (Lone and Mir, 2019; Rasjid et al., 2017). During the transfer of evidence, hash functions do not provide tamper-proof resistance of digital evidence from malicious participants or investigators in a way that guarantees transparency, traceability, and non-repudiation.

By leveraging the inherent properties of blockchain technology, the entire chain of custody lifecycle in IoT digital forensics can guarantee transparency, tamper-resistance, and verifiability. The majority of primary studies in this SLR [PS1], [PS2], [PS3], [PS5], [PS6], [PS7], [PS8], [PS9], [PS12], [PS13], [PS14], [PS15], [PS16], use blockchain to address issues surrounding evidence traceability, auditability, and accountability due to the secure and immutable nature of blocks and transactions. As new evidence is collected and added to the storage medium block, both public and permissioned blockchain distributed ledgers ensure an immutable record of the evidence log and guarantee evidence integrity by detecting any modification or alteration in the evidence chain. When the evidence has been submitted, it cannot be modified but can only be updated by submitting the latest evidence [PS7]. The blockchain is used to certify the authenticity and legitimacy of the procedures used to gather, store, and transfer digital evidence, as well as, to provide a comprehensive view of all the interactions in the chain of custody [PS1], [PS2], [PS3], [PS7], [PS8]. Primary study [PS12] conveys how the chain of custody forms the forensic link of evidence sequence of control, transfer, and analysis to preserve evidence integrity and prevent its contamination.

- *Data integrity and Data provenance*— The decentralized nature of blockchain technologies can well match the needs of integrity and provenances of evidence collecting in digital forensics across jurisdictional borders [PS1], [PS4], [PS5], [PS6], [PS7], [PS8], [PS9], [PS10], [PS11], [PS12], [PS13], [PS14], [PS15], [PS16]. These studies leverage blockchain for the provenance of any event or data collected to be traced back to where it initially entered the process in question, hence increasing transparency of the audit trail. To ensure data integrity, primary studies [PS5], [PS6], and [PS15], propose the hash value of the evidence data be signed by the data uploader or participants before it is stored on the blockchain. Primary studies [PS7], [PS12], go further by storing the value derived from the hash value of the evidence file name combined with the hash value of the evidence on the blockchain.

Data provenance solutions combined with blockchain technology are one way to make data more trustworthy by providing tamper-proof information about the origin and history of evidence data records. Considering the Internet of Vehicles (IoV) forensics, primary studies [PS9], [P10] describe how investigators can use the blockchain secure provenance of evidence to establish facts about road traffic incidents, therefore eliminating the need for a trusted arbiter. Recording data provenance provides a foundation for assessing authenticity, enabling trust, and allowing reproducibility.

- *Privacy and identity anonymity*— Privacy and identity anonymity of participants and stakeholders remain a constant challenge especially in the realm of public blockchains like Bitcoin and Ethereum for digital forensic investigations since they rely on data being transparent and verifiable by every participant (Lone and Mir, 2019; Sigwart et al., 2019). Primary study [PS6], which utilizes a custom distributed public blockchain, proposed each blockchain transaction should contain the public keys of the involved participants in addition to hashes and signatures. However, the identities of the parties are not included in the evidence transaction. Only the blockchain escrow service has the mapping between identities and public keys. Other primary studies [PS2], [PS7], [PS10], [PS15], and [PS16], proposed the use of pseudo-identities to satisfy the anonymity of participants, stakeholders and evidence custodians using randomized cryptographic hashing techniques and Merkle signatures. To ensure the privacy and confidentiality of evidence data stored on the blockchain, primary study [PS15], [PS16], proposed authentication and access control mechanisms to prevent unauthorized entities from accessing blockchain evidence data. Primary study [PS15] provides a secure audit trail and authentication using group signatures. It ensures privacy and identity anonymity by leveraging anonymous authentication. It also achieves access control by utilizing ciphertext-policy attribute-based encryption.

6.3. RQ3. How efficient are the blockchain-based IoT forensic investigation process models?

Due to the inherent peer-to-peer and distributed nature of blockchain-based transactions, the implementation of blockchain is considered resource-intensive and expensive. Currently, there are no conventional tools and standards that can provide performance evaluations for different blockchain solutions (Zheng et al., 2019). However, performance benchmark frameworks for analysing blockchains such as *Blockbench* (for permissioned blockchains) (Dinh et al., 2017) and *Hyperledger Caliper* (for mixed blockchain solutions) (Hyperledger Caliper, 2021) have been proposed. Empirical studies on the performance evaluation of blockchain platforms have been carried out, especially for permissioned blockchain platforms and are well documented in the study by Dabbagh et al. (2021). Performance evaluation of blockchain platforms measures different metrics including execution time, latency, throughput, energy consumption, and scalability.

In our SLR, the performance evaluations for the different proposed blockchain-based IoT forensic investigation process models vary significantly and are measured in similar ways including the cost, privacy, and security benefit of their implementation. This is due to the different consensus algorithms and performance characteristics of public and permissioned-based blockchain platforms used by each proposed model. To increase performance, only the evidence information (signature hashes and metadata) is stored on the blockchain, while the raw evidence data is stored on a trusted storage platform or off-chain database [PS3], [PS5], [PS6], [PS7], [PS15]. Primary study [PS4] utilizes hash functions along with Merkle signatures to reduce cost and data size written to public blockchains. If the computed Merkle root and the hash value which is saved on the Ethereum platform match, the investigators know with certainty that the data centre has provided valid or tamper-proof IoT hash data. They know that the existence of the transaction in the blockchain has been validated by different multi-chain miners and that there is an extensive Proof-of-Work (PoW) or computation time ensuring the integrity of the hash data. The platform infrastructure of the Hyperledger Composer prototype used in [PS13] outperforms that of a permissioned-based Ethereum prototype used in [PS15] in terms of all performance metrics. Similarly, experiments conducted in [PS7], which uses the *Practical Byzantine Fault Tolerance* (PBFT) consensus algorithm, show that the IoT forensic investigation process model outperforms the model proposed in [PS15] which uses *Clique*, a kind of *Proof of Activity* (PoA), as the consensus mechanism based on communication overhead.

A comparison of performance evaluation results between [PS13] and [PS16] using *Hyperledger Caliper* as a performance evaluation benchmark showed significant differences. The results show that in a 2-organization-1-peer network model with each *Send Rate* of 49tps after 9 and 10 rounds of tests respectively, [PS16] attained higher throughput and lower latency (*Throughput* =30tps and *Average Latency* =*9.86 s*) compared to [PS13] (*Throughput* =13tps and *Average Latency* =*11.85 s*). It is worth noting that the primary study [PS16] uses both Hyperledger Fabric and permission based Ethereum platform (Go Ethereum/Geth) for their prototype simulation. However, details of the consensus algorithms' impact on performance analysis in both experiments were not taken into consideration.

In primary studies [PS8] and [PS16], the cost-effectiveness associated with gas consumption to cover 800 pieces of evidence was conducted. The results highlighted that the price to pay for gas consumption for the prototype proposed in [PS16] is approximately the same compared to that of [PS8] (0.000000048 Ethereum and 0.00000005 Ethereum respectively). Both experiments assumed the denomination of Gwei as 1 Gwei is equivalent to 0.000000001 Ethereum and 10 Gwei per gas is used for fast transmission. However, the block size increased from 0.5 KB to 3.34 KB and 0.4 to 1.34 KB for primary studies [PS16] and [PS8] respectively. In their cost analysis, primary study [PS4] proposed the use of multi-chain (Stellar and EOS) blockchain platforms as a cheaper alternative to Ethereum.

In summary, the overall performance of each proposed blockchain-based IoT forensic investigation process model could impact the choice of selection for IoT forensic investigations. Each model has its performance characteristics under various conditions, and one may outperform the other in terms of a specific performance metric. However, the utmost importance of each model is to ensure, authenticity, integrity, transparency, and a secure audit trail of digital evidence as it moves along different stages of hierarchy in the chain of custody during the forensic investigation process. The comparison of the performance evaluations conducted by 11 out of 16 selected primary studies is summarised in Table 4.

7. Open issues and future research directions

Based on the findings and discussion of results (addressing RQ1, RQ2 and RQ3), we describe several open issues, challenges, and future research directions.

- *Security issues*—The majority of the proposed blockchain-based IoT forensic investigation process models are focused on solving issues associated with maintaining the integrity and authenticity of digital evidence generated by billions of IoT devices that need to be stored and accessed during a digital forensic investigation for its admissibility in a court of law. They guarantee data provenance, privacy, availability, transparency, traceability, trust, and continuous integrity of IoT forensic artefacts and evidential data. The security of the underlying blockchain infrastructure of the proposed models remains an issue and may be subject to security attacks. It can be observed from Table 3, that only a few primary studies implemented access control mechanisms to address the issues of unauthorised access by participants, privacy, and identity anonymity. Details of identity vulnerabilities (replay, impersonation and Sybil attacks) where an adversary attempts to compromise the identity of blockchain users are well documented in the study by Dasgupta et al. (2019). Several real attacks on blockchain systems were covered extensively by Li et al. (2020). The blockchain infrastructures can also be overloaded by DDoS (Distributed Denial of Service) attacks which can deplete huge resources of the network and make legitimate users unable to respond to service requests promptly (Alkurdi et al., 2019; Zheng et al., 2019). Due to computation costs, a handful of primary studies proposed off-chain data storage of IoT evidence data while evidence information is stored on the blockchain. Hence, off-chain data storages are susceptible to malicious attacks, as they do not take advantage of the security, reliability, and transparency properties of the blockchain.

Therefore, it is essential that studies that include rigorous security testing and evaluation be carried out on these proposed models to ensure resilience against attacks and review their impact on the soundness of IoT forensic investigations.

- *Performance evaluation issues*— The performance evaluation results only highlight the differences between the execution layers of these blockchain-based IoT forensic investigation process models. The details and effect of the consensus algorithm on the performance evaluation of these models were not analysed and presented. A handful of proposed models did not describe the specific consensus algorithm utilized either. Moreover, each prototype proposed in the primary studies did not highlight the versions of Ethereum, Hyperledger Fabric/Composer or other blockchain platforms utilized. Studies have shown the differences between blockchain versions (Dinh et al., 2017; Nasir et al., 2018; Pongnumkul et al., 2017) and consensus algorithms (Hao et al., 2018) impact performance metrics. Similarly, performance evaluations based on scalability issues, the increase in the size of the blockchain and the number of participants (nodes) interacting with evidence data on the

Table 4
Summary of performance metrics results from selected primary studies.

Primary Study (PS)	Performance Metrics								
	Blockchain category	Blockchain Platform	Consensus Algorithm	Latency	Execution time	Throughput	Energy consumption	Computational cost	Scalability
[PS4]	Public	Multi-chain	Proof of Stake (PoS)	✗	✓	✗	✗	✓	✗
[PS6]	Public	Ethereum	Proof of Work (PoW)	✗	✓	✗	✓	✗	✗
[PS7]	Permissioned	Mixed/Multi-chain	Practical Byzantine Fault Tolerance (PBFT)	✗	✗	✗	✗	✗	✓
[PS8]	Permissioned	Ethereum (Geth)	Proof of Work (PoW)	✗	✗	✓	✓	✓	✗
[PS9]	Public	Custom	Not reported	✗	✓	✗	✓	✓	✗
[PS11]	Public	Ethereum	Not reported	✓	✗	✓	✗	✗	✗
[PS12]	Permissioned	Ethereum (Geth)	Raft and IBFT	✗	✓	✗	✗	✗	✓
[PS13]	Permissioned	Hyperledger Composer/ Fabric	Not reported	✓	✗	✓	✗	✗	✗
[PS14]	Permissioned	Ethereum	Proof of Work (PoW)	✗	✗	✗	✗	✗	✓
[PS15]	Permissioned	Ethereum (Geth)	Clique-Proof of Activity (PoA)	✓	✓	✓	✗	✓	✗
[PS16]	Permissioned	Hyperledger Fabric & Ethereum (Geth)	Not reported	✓	✗	✓	✓	✓	✗

blockchain platform were addressed only in a few of the primary studies [PS1],[PS7], [PS8], [PS11], [PS12]. This shows that further performance evaluation research needs to be conducted for the proposed models as this research area of blockchain application to IoT forensics is still in its nascent stage.

8. Conclusion

In this paper, we focused on blockchain-based IoT forensic investigation process models. We conducted a systematic literature review of the latest models and examined how these proposed models are designed to improve the evidence chain of custody, maintain privacy, guarantee integrity, provenance, traceability, and verification of evidence collected and stored during the investigation process. Our findings show that most of the blockchain-based IoT forensic investigation process models are used to improve the evidence chain of custody, data integrity, data provenance, privacy, and identity anonymity in that order. Our study also revealed that the majority of the proposed models are based on permissioned blockchain. We reviewed the efficiency of selected proposed models and prototype proofs-of-concept, based on their performance evaluation results and metrics. Finally, we highlighted challenges, open issues, and potential research directions to address them. Our potential future research agenda includes an empirical evaluation of the security of these proposed blockchain-based IoT forensic investigation models and other newer models in an attempt to address the security issues described in Section 7.

Primary studies

[PS1] S. Li, T. Qin, G. Min, Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems, IEEE Trans. Comput. Soc. Syst. 6 (2019) 1433–1441. https://doi.org/10.1109/TCSS.2019.2927431.

[PS2] D.P. Le, H. Meng, L. Su, S.L. Yeo, V. Thing, BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy, in: IEEE Reg. 10 Annu. Int. Conf. Proceedings/ TENCON, 2019. https://doi.org/10.1109/TENCON.2018.8650434.

[PS3] S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros, E. Bellini, C. Pavue, Blockchain solutions for forensic evidence preservation in iot environments, in: Proc. 2019 IEEE Conf. Netw. Softwarization Unleashing Power Netw. Softwarization, NetSoft 2019, 2019. https://doi.org/10.1109/NETSOFT.2019.8806675.

[PS4] S. Mercan, M. Cebe, E. Tekiner, K. Akkaya, M. Chang, S. Uluagac, A Cost-efficient IoT Forensics Framework with Blockchain, in: IEEE Int. Conf. Blockchain Cryptocurrency, ICBC 2020, 2020. https://doi.org/10.1109/ICBC48266.2020.9169397.

[PS5] M. Hossain, R. Hasan, S. Zawoad, Probe-IoT: A public digital ledger based forensic investigation framework for IoT, in: INFOCOM 2018 - IEEE Conf. Comput. Commun. Work., Institute of Electrical and Electronics Engineers Inc., 2018: pp. 1–2. https://doi.org/10.1109/INFCOMW.2018.8406875.

[PS6] M. Hossain, Y. Karim, R. Hasan, FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger, in: 2018 IEEE Int. Congr. Internet Things, IEEE, 2018: pp. 33–40. https://doi.org/10.1109/ICIOT.2018.00012.

[PS7] Z. Tian, M. Li, M. Qiu, Y. Sun, S. Su, Block-DEF: A secure digital evidence framework using blockchain, Inf. Sci. (Ny). (2019). https://doi.org/10.1016/j.ins.2019.04.011.

[PS8] J.H. Ryu, P.K. Sharma, J.H. Jo, J.H. Park, A blockchain-based decentralized efficient investigation framework for IoT digital forensics, J. Supercomput. 75 (2019) 4372–4387. https://doi.org/10.1007/s11227-019-02779-9.

[PS9] M. Hossain, R. Hasan, S. Zawoad, Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (IoV), in: Proc. - 2017 IEEE 2nd Int. Congr. Internet Things, ICIOT 2017, 2017. https://doi.org/10.1109/IEEE.ICIOT.2017.13.

[PS10] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles, IEEE Commun. Mag. (2018). https://doi.org/10.1109/MCOM.2018.1800137.

[PS11] M. Sigwart, M. Borkowski, M. Peise, S. Schulte, S. Tai, Blockchain-based Data Provenance for the Internet of Things, in: Proc. 9th Int. Conf. Internet Things, ACM, New York, NY, USA, 2019: pp. 1–8. https://doi.org/10.1145/3365871.3365886.

[PS12] L. Ahmad, S. Khanji, F. Iqbal, F. Kamoun, Blockchain-based chain of custody: Towards real-time tamper-proof evidence management, in: ACM Int. Conf. Proceeding Ser., 2020. https://doi.org/10.1145/3407023.3409199.

[PS13] A.H. Lone, R.N. Mir, Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer, Digit. Investig. 28 (2019) 44–55. https://doi.org/10.1016/j.diin.2019.01.002.

[PS14] S. Chen, C. Zhao, L. Huang, J. Yuan, M. Liu, Study and implementation on the application of blockchain in electronic evidence generation, Forensic Sci. Int. Digit. Investig. 35 (2020) 301001. https://doi.org/10.1016/j.fsidi.2020.301001.

[PS15] M. Li, C. Lal, M. Conti, D. Hu, LEChain: A blockchain-based lawful evidence management scheme for digital forensics, Futur. Gener. Comput. Syst. 115 (2021) 406–420. https://doi.org/10.1016/j.future.2020.09.038.

[PS16] G. Kumar, R. Saha, C. Lal, M. Conti, Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications, Futur. Gener. Comput. Syst. 120 (2021) 13–25. https://doi.org/10.1016/j.future.2021.02.016.

Declaration of competing interest

The authors acknowledge there is no conflict of interest.

Data availability

No data was used for the research described in the article.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

Achimugu, P., Selamat, A., Ibrahim, R., Mahrin, M.N.R., 2014. A systematic literature review of software requirements prioritization research. Inf Softw Technol. https://doi.org/10.1016/j.infsof.2014.02.001.

Akinbi, A., Berry, T., 2020. Forensic investigation of google assistant. SN Comput Sci 1, 272. https://doi.org/10.1007/s42979-020-00285-x.

Alenezi, Ahmed, Atlam, H., Alsagri, R., Alassafi, M., Wills, G., 2019. IoT forensics: a state-of-the-art review, challenges and future directions. In: Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk. SCITEPRESS - Science and Technology Publications, pp. 106–115. https://doi.org/10.5220/0007905401060115.

Alenezi, A., Atlam, H.F., Wills, G.B., Alsagri, R., Alassafi, M.O., 2019. IoT forensics: a state-of-the-art review, challenges and future directions. In: COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk.

Alkurdi, F., Elgendi, I., Munasinghe, K.S., Sharma, D., Jamalipour, A., 2019. Blockchain in IoT security: a survey. In: 2018 28th International Telecommunication Networks and Applications Conference, ITNAC 2018. https://doi.org/10.1109/ATNAC.2018.8615409.

Atlam, H.F., El-Din Hemdan, E., Alenezi, A., Alassafi, M.O., Wills, G.B., 2020. Internet of Things Forensics: A Review. https://doi.org/10.1016/j.iot.2020.100220. Internet of Things 100220.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G., 2019. SoK. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. ACM, New York, NY, USA, pp. 183–198. https://doi.org/10.1145/3318041.3355458.

BBC, 2018. Amazon Asked to Share Echo Data in US Murder Case [WWW Document]. BBC.co.uk. https://www.bbc.co.uk/news/technology-46181800. accessed 5.3.20.

Hyperledger Caliper, 2021. Hyperledger Caliper [WWW Document]. https://www.hyperledger.org/use/caliper. accessed 4.24.21.

Casino, F., Dasaklis, T.K., Patsakis, C., 2019. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Inf. https://doi.org/10.1016/j.tele.2018.11.006.

Chen, S., Zhao, C., Huang, L., Yuan, J., Liu, M., 2020. Study and implementation on the application of blockchain in electronic evidence generation. Forensic Sci. Int.: Digit. Invest. 35, 301001. https://doi.org/10.1016/j.fsidi.2020.301001.

Chernyshev, M., Zeadally, S., Baig, Z., Woodward, A., 2018. Internet of things forensics: the need, process models, and open issues. IT Prof 20, 40–49. https://doi.org/10.1109/MITP.2018.032501747.

Chung, H., Park, J., Lee, S., 2017. Digital forensic approaches for Amazon Alexa ecosystem. Digit. Invest. 22, S15–S25. https://doi.org/10.1016/j.diin.2017.06.010.

Conoscenti, M., Vetro, A., De Martin, J.C., 2016. Blockchain for the Internet of Things: a systematic literature review. In: Proceedings of IEEE/ACS International Conference on Computer Systems and Applications. AICCSA. https://doi.org/10.1109/AICCSA.2016.7945805.

Conti, M., Dehghantanha, A., Franke, K., Watson, S., 2018. Internet of Things security and forensics: challenges and opportunities. Future Generat. Comput. Syst. 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060.

Dabbagh, M., Choo, K.-K.R., Beheshti, A., Tahir, M., Safa, N.S., 2021. A survey of empirical performance evaluation of permissioned blockchain platforms: challenges and opportunities. Comput. Secur. 100, 102078. https://doi.org/10.1016/j.cose.2020.102078.

Dasgupta, D., Shrein, J.M., Gupta, K.D., 2019. A survey of blockchain from security perspective. J. Bank. Finan. Technol. 3, 1–17. https://doi.org/10.1007/s42786-018-00002-6.

Dawson, L., Akinbi, A., 2021. Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study. Forensic Sci. Int.: Reports 3, 100198. https://doi.org/10.1016/j.fsir.2021.100198.

Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.L., 2017. BLOCKBENCH: a framework for analyzing private blockchains. In: Proceedings of the ACM SIGMOD International Conference on Management of Data. https://doi.org/10.1145/3035918.3064033.

Hao, Y., Li, Y., Dong, X., Fang, L., Chen, P., 2018. Performance analysis of consensus algorithm in private blockchain. In: IEEE Intelligent Vehicles Symposium, Proceedings. https://doi.org/10.1109/IVS.2018.8500557.

Hauser, C., 2017. In: Connecticut Murder Case, a Fitbit Is a Silent Witness [WWW Document]. New York Times. https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html. accessed 5.4.20.

Hegarty, R.C., Lamb, D.J., Attwood, A., 2014. Digital evidence challenges in the internet of things. In: Proceedings of the Tenth International Network Conference (INC) 2014, pp. 162–220.

Hossain, M., Hasan, R., Zawoad, S., 2018a. Probe-IoT: a public digital ledger based forensic investigation framework for IoT. In: INFOCOM 2018 - IEEE Conference on Computer Communications Workshops. Institute of Electrical and Electronics Engineers Inc., pp. 1–2. https://doi.org/10.1109/INFCOMW.2018.8406875

Hossain, M., Karim, Y., Hasan, R., 2018b. FIF-IoT: a forensic investigation framework for IoT using a public digital ledger. In: 2018 IEEE International Congress on Internet of Things (ICIOT). IEEE, pp. 33–40. https://doi.org/10.1109/ICIOT.2018.00012.

Hou, J., Li, Y., Yu, J., Shi, W., 2020. A survey on digital forensics in internet of things. IEEE Internet Things J. 7, 1–15. https://doi.org/10.1109/JIOT.2019.2940713.

Kebande, V.R., Ray, I., 2016. A generic digital forensic investigation framework for internet of things (IoT). In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, pp. 356–362. https://doi.org/10.1109/FiCloud.2016.57.

Kebande, V.R., Karie, N.M., Venter, H.S., 2017. Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures. In: 2017 1st International Conference on Next Generation Computing Applications (NextComp). IEEE, pp. 54–60. https://doi.org/10.1109/NEXTCOMP.2017.8016176.

Kebande, V.R., Mudau, P.P., Ikuesan, R.A., Venter, H.S., Choo, K.-K.R., 2020. Holistic digital forensic readiness framework for IoT-enabled organizations. Forensic Sci. Int.: Reports. https://doi.org/10.1016/j.fsir.2020.100117.

Khan, M.A., Salah, K., 2018. IoT security: review, blockchain solutions, and open challenges. Future Generat. Comput. Syst. 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022.

Kitchenham, B., Charters, S., 2007. Guidelines for performing systematic literature reviews in software engineering. In: Technical Report, Ver. 2.3 EBSE Technical Report. EBSE. https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

Li, J., Wu, J., Chen, L., 2018. Block-secure: blockchain based scheme for secure P2P cloud storage. Inf. Sci. https://doi.org/10.1016/j.ins.2018.06.071.

Li, S., Li, S., Choo, K.-K.R., Sun, Q., Buchanan, W.J., Cao, J., 2019a. IoT forensics: amazon echo as a use case. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2019.2906946, 1–1.

Li, S., Qin, T., Min, G., 2019b. Blockchain-based digital forensics investigation framework in the internet of things and social systems. IEEE Trans. Comput. Soc. Syst. 6, 1433–1441. https://doi.org/10.1109/TCSS.2019.2927431.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., 2020. A survey on the security of blockchain systems. Future Generat. Comput. Syst. 107, 841–853. https://doi.org/10.1016/j.future.2017.08.020.

Lone, A.H., Mir, R.N., 2019. Forensic-chain: blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digit. Invest. 28, 44–55. https://doi.org/10.1016/j.diin.2019.01.002.

Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., Bakhtiari Bastaki, B., 2021. The complexity of internet of things forensics: a state-of-the-art review. Forensic Sci. Int.: Digit. Invest. 38, 301210. https://doi.org/10.1016/j.fsidi.2021.301210.

MacDermott, A., Baker, T., Shi, Q., 2018. Iot forensics: challenges for the Ioa era. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, pp. 1–5. https://doi.org/10.1109/NTMS.2018.8328748.

Nasir, Q., Qasse, I.A., Abu Talib, M., Nassif, A.B., 2018. Performance analysis of hyperledger fabric platforms. Secur. Commun. Network. https://doi.org/10.1155/2018/3976093.

O'Shaughnessy, S., Keane, A., 2013. Impact of cloud computing on digital forensic investigations. In: IFIP Advances in Information and Communication Technology. https://doi.org/10.1007/978-3-642-41148-9_20.

Pongnumkul, S., Siripanpornchana, C., Thajchayapong, S., 2017. Performance analysis of private blockchain platforms in varying workloads. In: 2017 26th International Conference on Computer Communications and Networks, ICCCN. https://doi.org/10.1109/ICCCN.2017.8038517, 2017.

Rasjid, Z.E., Soewito, B., Witjaksono, G., Abdurachman, E., 2017. A review of collisions in cryptographic hash function used in digital forensic tools. Procedia Comput. Sci. 116, 381–392. https://doi.org/10.1016/j.procs.2017.10.072.

Salman, T., Zolanvari, M., Erbad, A., Jain, R., Samaka, M., 2019. Security services using blockchains: a state of the art survey. In: IEEE Communications Surveys and Tutorials. https://doi.org/10.1109/COMST.2018.2863956.

Servida, F., Casey, E., 2019. IoT forensic challenges and opportunities for digital traces. Digit. Invest. 28, S22–S29. https://doi.org/10.1016/j.diin.2019.01.012.

Sigwart, M., Borkowski, M., Peise, M., Schulte, S., Tai, S., 2019. Blockchain-based data provenance for the internet of things. In: Proceedings of the 9th International Conference on the Internet of Things. ACM, New York, NY, USA, pp. 1–8. https://doi.org/10.1145/3365871.3365886.

Statista, 2020. IoT Connected Devices Worldwide 2030 [WWW Document]. Statista

Research Department.
Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutor. 22, 1191–1221. https://doi.org/10.1109/COMST.2019.2962586.
Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., Choo, K.-K.R., 2020. A systematic literature review of blockchain cyber security. Digit. Commun. Netw. 6, 147–156. https://doi.org/10.1016/j.dcan.2019.01.005.
Wohlin, C., 2014. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: ACM International Conference Proceeding Series. https://doi.org/10.1145/2601248.2601268.
Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.M.A., Hong, C.S., 2019. Internet of things forensics: recent advances, taxonomy, requirements, and open challenges. Future Generat. Comput. Syst. 92, 265–275. https://doi.org/10.1016/j.future.2018.09.058.
Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., 2016. Where is current research on Blockchain technology? - a systematic review. PLoS One. https://doi.org/10.1371/journal.pone.0163477.
Zawoad, S., Hasan, R., 2015. FAIoT: towards building a forensics aware eco system for the internet of things. In: 2015 IEEE International Conference on Services Computing. IEEE, pp. 279–284. https://doi.org/10.1109/SCC.2015.46.
Zhang, X., Choo, K.-K.R., Beebe, N.L., 2019. How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2019.2912118, 1–1.
Zheng, X., Zhu, Y., Si, X., 2019. A survey on challenges and progresses in blockchain technologies: a performance and security perspective. Appl. Sci. 9, 4731. https://doi.org/10.3390/app9224731.
Zhu, L., Wu, Y., Gai, K., Choo, K.K.R., 2019. Controllable and trustworthy blockchain-based cloud data management. Future Generat. Comput. Syst. https://doi.org/10.1016/j.future.2018.09.019.