Hindawi
Security and Communication Networks
Volume 2022, Article ID 4490757, 14 pages
https://doi.org/10.1155/2022/4490757

Research Article

Research on IoT Forensics System Based on Blockchain Technology

Guangjun Liang,[1,2,3] Jianfang Xin ,[4] Qun Wang,[1,2] Xueli Ni,[1,2,3] and Xiangmin Guo[1,2,3]

[1] *Department of Computer Information and Cyber Security, Jiangsu Police Institute, Nanjing, China*
[2] *Engineering Research Center of Electronic Data Forensics Analysis, Jiangsu Province, Nanjing, China*
[3] *Key Laboratory of Digital Forensics, Department of Public Security of Jiangsu Province, Nanjing, China*
[4] *School of Intelligent Engineering, Nanjing Institute of Railway Technology, Nanjing, China*

Correspondence should be addressed to Jianfang Xin; xinjfang@163.com

Received 20 August 2021; Accepted 4 May 2022; Published 15 June 2022

Academic Editor: Gautam Srivastava

In recent years, mobile edge computing (MEC) has become a research hotspot in academia. The Internet of Things (IoT) is an excellent way to build the infrastructure required for a MEC environment. Its rich digital tracking repository can provide insights into people's daily activities at home and elsewhere. Meanwhile, due to the open connectivity of the Internet of things devices, they can easily become the target of network attacks and be used by criminals as criminal tools. As a result, civil and criminal cases have increased year by year. This article conducts in-depth research on IoT forensics. By comparing its difference with traditional digital forensics (DF), the definition of IoT forensics is given. We have systematically sorted out the research results since the concept of IoT forensics was proposed in 2013 and proposed a generalized IoT forensics model. By studying blockchain technology and introducing it into the IoT forensics framework, a blockchain-based IoT forensics architecture is further proposed. Further, an alliance chain IoT forensics system is proposed. From the perspective of the data provider and the data visitor, the process of evidence storage and forensics of the IoT system is discussed. Finally, taking Unmanned Aerial Vehicle (UAV) forensics as an example, we give an experiment of IoT forensics analysis.

1. Introduction

The use of the IoT in our daily life leads to two phenomena. First, the use of intelligent Internet of things related devices makes people leave digital traces on these devices, and the data of users' daily activities can be obtained by tracing the personal information stored in the database [1]. Secondly, the number of cases of online fraud is increasing year by year, and various Internet of things devices may become network attack objects or criminal tools. The security vulnerabilities in the IoT system can easily be used by criminals as a means of remote control. In short, public security organs urgently need Internet of things forensics workers to help determine the key information of the case.

The IoT technology can send and receive information between two or more interconnected devices through the internet. As IoT is widely used in various industries such as industry, commerce, and agriculture, IoT devices such as smart sensors have brought huge security risks to users. Liang and Kim [2] conducted research on IoT security, discussed applications in edge computing and blockchain scenarios, and pointed out that machine learning may be a better solution. Regarding IoT platforms and systems, Zhou [3] discussed the lessons learned from these bugs. Miloslavskaya and Tolstoy [4] were concerned about the typical attack problems of IoT assets, and they proposed to find possible security vulnerabilities through intelligent security protection of the Internet of things.

The necessity for scholars to study data forensics technology is that the increase of Internet of things devices increases computer-related crimes. Al-Masri et al. [5] introduced a Fog-based IoT Forensics Framework (FoBI).

Some key problems in digital forensics (DF) are studied, and corresponding solutions are given. The data forensics investigation process includes three steps: data collection, investigation, and investigation results. Investigators further compared digital evidence on different devices. Silvarajoo et al. [6] use appropriate case management tools hosted on the Web to simplify information collection and consolidate data. Because the data formats of different platforms are quite different, the lack of a unified standard has brought great trouble to the follow-up investigation and evidence collection. A management strategy for unified format and shared data is proposed. To assist the FBI in identifying suspects, Elhoseny et al. [7] proposed an optimal deep learning-based convolutional neural network (ODL-CNN).

Due to the distributed storage, decentralized management, and nontampering characteristics of blockchain, this emerging technology can be widely used in important industries such as medical treatment, commerce, information technology sector, and agriculture. Su et al. [8] discussed the sharing scheme in the financial field and pointed out that the most difficult to solve is the security of data-sharing. A data sharing model based on blockchain is proposed, and the technical scheme in the process of establishing the model is given in detail. Sathya et al. [9] focus on the blockchain-based food supply chain field, introduce smart contracts, and propose a supply chain management architecture based on Ethereum. In the food supply chain, there are fewer external attacks, and more research should be done on food traceability, prevention of forged data, server tampering, and other malicious behaviors. Agyekum et al. [10] proposed a blockchain-based proxy method to protect cloud data sharing through encryption. The data owner can use identity encryption to send the data to the cloud, and the agent can regrant the access rights of legal users. The blockchain-based system model is conducive to the decentralization of data sharing, relieving the pressure of big data processing in centralized systems, and is also conducive to the privacy protection of personal data.

Similarly, blockchain also has many applications in the DF of IoT. Kumar et al. [11] studied the issue of cross-border cloud forensics and proposed a blockchain customized IoT framework for DF, which is called Internet of Forensics (IoF). A transparent forensic investigation process was disclosed, taking into account the equipment involving multistakeholders. Existing digital forensics blockchain models tend to have weak security and less consideration for the privacy protection of stakeholders. Li et al. [12] conducted research on the legality of blockchain forensics. The research involves such links as evidence acquisition, evidence fixation, evidence analysis, and evidence presentation, as well as evidence supplementation and evidence circulation. The problem of weak security does not only appear in digital forensics but also in other blockchain systems. Li et al. [13] further study the security issues of blockchain. For each link in the blockchain system, the security risks and security solutions for the hidden risks are discussed separately.

This paper summarizes the research background and significance of IoTF. A blockchain-based IoT architecture is proposed, including an interface layer that can interact with applications. Then, the research background of blockchain technology is discussed, and an IoTF system based on an alliance chain is proposed. The previous research results of this paper were published in the ICAIS 2021 conference collection Advances in Artificial Intelligence and Security [14]. On this basis, we have an in-depth discussion of blockchain technology and further, propose an IoT forensics framework based on blockchain technology. By using the consortium chain idea, IoT terminal, IoT centralized devices, Regulatory department, Judicial department, and Insurance company are integrated into the forensics framework. For a more detailed explanation, we give application examples and flowcharts. Finally, we give a common example of IoTF, drone forensics, to help readers better understand our ideas.

The remaining part of the paper is organized as follows. Section 2 describes IoTF and DF. Section 3 is the research status of IoTF. Blockchain infrastructure and data structure are given in Section 4. The fifth part discusses the design of the blockchain-based IoTF system. Section 6 concludes the paper.

2. IoT Forensics and Digital Forensics

A table summarizing the acronym used in the paper is presented in Table 1.

2.1. What Is DF. At the first International Conference of Computer Investigation Experts (ICCIE) held in the United States in 1991, the concept of “computer evidence” was first put forward. Computer evidence is information stored in electronic form that can be identified, restored, extracted, saved, reported, and made into legal evidence.

The National People’s Congress deliberated and approved the draft amendment to the Criminal Procedure Law in 2012, and the new Criminal Procedure Law was formally implemented in 2013. This is the first time that my country’s law has included “electronic data” in the types of evidence. At the 28th meeting of the Standing Committee of the Eleventh National People’s Congress on August 31 of the same year, it was decided to make the following amendments to the “Civil Procedure Law of the People’s Republic of China,” adding the type of evidence “electronic data,” and it came into effect on January 1, 2015.

The Supreme People’s Court issued the newly amended “Several Provisions of the Supreme People’s Court on Evidence in Civil Litigation” in 2019, which will come into effect on May 1, 2020. Among them, the types of electronic data are detailed, including five types of various forms:

(1) Information published on web platforms, such as webpages, blogs, and microblogs.

(2) Application communication information of mobile phones, such as SMS, video communication, email, and so on.

(3) Electronic personal information of users, such as identity authentication information, electronic transaction information, communication records, etc.

Table 1: Table summarizing the acronym used in the paper.

Acronym	Explanation
MEC	Mobile edge computing
IoT	Internet of things
FoBI	Fog-based IoT forensics framework
ODL-CNN	Optimal deep learning-based convolutional neural network
IoF	Internet of forensics
ICCIE	International conference of computer investigation experts
DF	Digital forensics
USB	Universal serial bus
JPG	Joint picture group
MP3	Moving picture experts group audio layer-3
MP4	Mobile pentium 4
RFID	Radio frequency identification
EDFIM	Enhanced digital forensic investigation model
DFIM	Digital forensic investigation model
FSAC	Forensic state acquisition controller
FSIoT	Forensic status of the Internet of things
IoA	Internet of everything
PoW	Proof of work
PoS	Proof of stake
DPoS	Delegated proof of stake
PBFT	Practical byzantine fault tolerance
UAV	Unmanned aerial vehicle

(4) Electronic documents, pictures, films, and other electronic documents.

(5) Other information that can prove the facts of the case that is stored, processed, and transmitted in digital form.

Definition 1. Digital forensics is also called electronic data forensics, and its scope includes computer forensics, mobile phone forensics, network forensics, server forensics, etc. It is a process in which public security organs and judicial organs use computer-related technologies to identify, collect, fix, analyze, present, and preserve digital evidence extracted from electronic devices, thereby helping to reconstruct, reproduce, and prove criminal facts.

With the use of digital evidence in criminal law, civil law, and criminal procedure law more and more in-depth, the importance of digital forensics has gradually become prominent. In September 2016, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security issued the "Regulations on Several Issues Concerning the Collection, Extraction, Review, and Judgment of Electronic Data in Criminal Cases" notice, which was officially implemented on October 1. The "Regulations" pointed out that Electronic data includes but is not limited to the following information and electronic files. The Regulations divide electronic data into four categories, basically following the aforementioned "Several Provisions of the Supreme People's Court on Evidence in Civil Litigation," which will not be repeated here.

In January 2019, the Ministry of Public Security issued a notice on the "Rules for Public Security Organs' Handling of Criminal Cases Electronic Data Collection Rules," which came into effect on February 1. The "Rules" point out that digital forensics includes but is not limited to the following:

(1) Collect and extract electronic data

(2) Electronic data inspection and investigation experiments

(3) Electronic data inspection and appraisal

Simply put, the digital forensics process is the process of converting digital evidence into a report form.

The main steps of the digital forensics process are shown in Figure 1.

By considering the concepts related to digital forensics, there are also computer forensics and IoT forensics. Comparing these three concepts, the concept of digital forensics has the largest category. Digital forensics mainly faces the forensics of digital devices. A computer, also known as a digital computer, is a typical digital device. Basically, IoT devices are also digital devices. Therefore, the scope of digital forensics includes computer forensics and IoTF.

2.2. IoT Forensics VS Traditional Digital Forensics. The IoT is designed as a network of intelligent, decision-making, and self-management systems, which has a great impact on DF. Because from the perspective of criminal liability caused by smart things in the IoT, IoT proposes many dimensions. These dimensions will affect the conventional practice of DF. IoT forensics may be different from traditional DF in the following aspects. Table 2 highlights these differences.

2.3. IoT Forensic. Internet of things forensics can collect, analyze, and find digital evidence of data in IoT devices on the premise of legal binding. However, IoT devices with limited cache capacity may be difficult to achieve these goals. Moreover, some devices that can only be connected locally cannot quickly transfer evidence to researchers. Finally, technology law enforcement agencies can confiscate computers, servers, and other equipment, but it is not so simple to set up the amount of Internet of things equipment required for a case investigation.

With the rapid development of Internet of things technology, data evidence extends from personal assets such as notebooks to broad Internet of things devices such as wearable devices. This brings new opportunities and challenges to researchers. Only some of the previous forensics methods and tools are available in the IoTF. There is an urgent need for new tools and regulations to innovate the forensics technology in the era of the IoT [15]. As IoT communication needs to be carried out under the support of protocols and standards, there are high requirements for equipment and evidence collection materials. In 2015, [16] first proposed the concept of the Internet of things forensics and improved Edewede Oriwoh's 1-2-3 regional method model. [15] discusses equipment level forensics, network forensics, and cloud forensics (see Figure 2).

2.4. Generalized IoT Forensics Model. This section proposes a generalized IoT forensics model which consists of three independent components: forensic scenarios, forensic

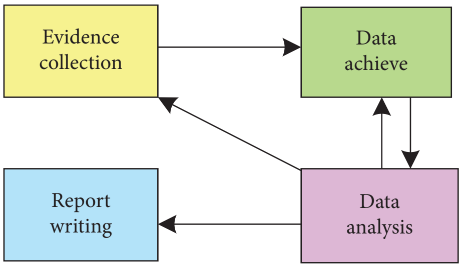

Figure 1: The main steps of the digital forensics process.

Table 2: IoT forensics VS traditional digital forensics.

	Traditional digital forensics	IoT forensics
Source of evidence	Traditional storage media such as computers, mobile phones, USB flash drives, cameras, and servers such as switches and routers	Smart terminals such as cars, drones, smartwatches, smart bracelets, smart sensors, smart industrial equipment, smart appliances, smart wearable devices
Equipment quantity	Tens of billions of magnitudes	Trillions of magnitude
Type of evidence	Electronic documents, standard format files (JPG, MP3, MP4, etc.)	Added a large number of nonstandard data files for IoT smart terminals
Evidence data size	Megabyte	Exabytes
Network type	Wired network, WIFI, Bluetooth, wireless network, internet, mobile communication network	Added RFID, wireless sensor network, Internet of things (Internet of vehicles, industrial Internet of things, etc.)
Protocol	Ethernet, wireless (802.11a/b/g/n), bluetooth, IPv4, IPv6, TCP/IP, etc.	RFID,TCP/IP,B/S和C/S,HTTP, Ajax,Websocket, MQTT,CoAP, etc.
Owner of the evidence (equipment)	Victims, suspects, related contacts	Anyone
Judicial	The relevant legislation is basically complete	The relevant legislation is not yet complete
Privacy	Infringement of citizens' privacy is less problematic	Legislation and borders are not clear, and privacy issues are involved

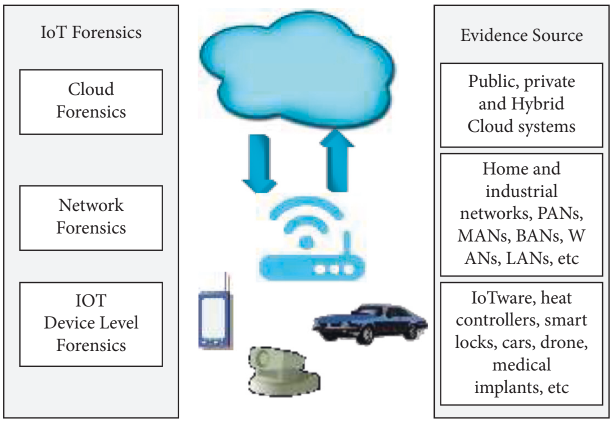
IoT Forensics
Cloud Forensics
Network Forensics
IOT Device Level Forensics
Evidence Source
Public, private and Hybrid Cloud systems
Home and industrial networks, PANs, MANs, BANs, WANs, LANs, etc
IoTware, heat controllers, smart locks, cars, drone, medical implants, etc

Figure 2: Three-tier IoT forensics model.

objects, and forensic processes (see Figure 3). The IoT forensics scene is very broad, and it can even be said to cover all aspects of our work and life. This confirms the importance of IoT forensics from another perspective. People will always leave traces in the IoT unknowingly, which will be an important starting point and breakthrough for digital forensics investigators. Although this will involve user privacy issues, we will discuss them in detail in the follow-up content.

Here, we use smart home, smart wear, industrial internet, and Internet of Vehicles as typical IoT forensics scenarios. All kinds of smart appliances in the smart home scene can be obtained for evidence, such as smart TVs, smart door locks, smart rice cookers, smart refrigerators, routers, and so on. Through the forensics of smart door locks, the information of the permanent population of the family can be obtained, and even the fingerprint information of the relevant personnel can be obtained directly. Through router forensics, you can obtain information such as the person and time of the wifi login user. Through smart TV forensics, you can obtain information such as family member composition, preferences, and living habits. The forensics of other smart appliances, such as smart rice cookers, smart refrigerators, etc., will also help the suspect's portrait to obtain clues to the case.

For forensics objects, we follow Edewede Oriwoh's model, which is divided into three levels: corresponding to the terminal forensics at the bottom, network forensics at the middle layer, and cloud forensics at the upper layer. The object of terminal forensics is the most extensive, and all IoT terminal devices are covered. Network forensics is an extension of terminal equipment forensics. The target is the network flow of all possible criminal computers, audit logs, and system logs. Cloud forensics refers to the collection of digital forensics data from cloud infrastructure. Terminal forensics and network forensics generally specifically refer to the collection of information from log files, data stored on disks, network traffic, and intrusion markers. The basic difference between terminal forensics and network forensics, and cloud forensics is that you can collect and analyze

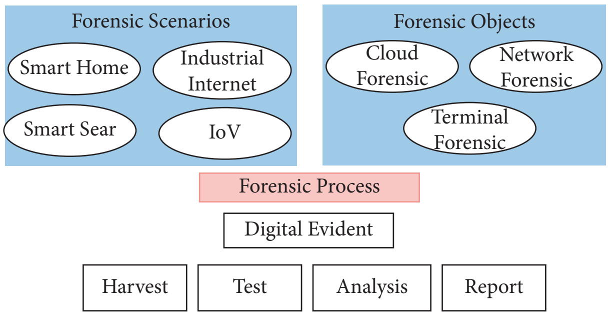

Figure 3: Generalized IoT forensics model.

information by simply entering the system using a local computer. However, when it comes to the cloud, the machine cannot be physically accessed; only certain parts of the computer can be accessed through the cloud application program interface. In addition, since cloud servers can be located in multiple countries, forensic data may also belong to multiple jurisdictions. The issue of jurisdiction cannot be ignored.

3. Research Status of Forensics in the Internet of Things

In 2013, Edewede Oriwoh et al. first proposed the concept of IoT forensics [15]. A 1-2-3 area method is proposed to be applied to DF research related to the IoT, which is the earliest IoT forensics model. After continuous improvement, in 2015, Shams Zawoad gave the definition of IoTF firstly [16]. Extend the DF to the category of IoT, study the DF process of IoT devices, and give an accurate definition of IoTF.

Aiming at the privacy issue of IoT forensics, Ana Nieto et al. conducted pioneering research. In 2016, Ana Nieto et al. published a long journal article on "digital witnesses" [17], which was the first journal article on forensics research on the Internet of Things. This article first 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. In 2017, Ana Nieto and others analyzed the enhanced digital forensic investigation model (EDFIM). By including the privacy protection requirements of the 1974 "US Privacy Act" and ISO/IEC 29100:2011 [18] in the entire investigation life cycle, a privacy-aware IoT forensics model (PROFIT) [19] is proposed.

In 2017, literature [20] discussed the key issues of IoT forensics from the perspective of IoT security. First, starting with the basic elements of IoT, it discussed the three-tier framework of IoT and the key issues of IoT forensics. Then it further reviewed the research and development of the forensic model of the IoT in recent years. Literature [21] considers the heterogeneity of devices in the IoT system and the lack of uniform standards. By taking forensics in three representative IoT application scenarios, smart homes, wearable devices, and smart cities, as examples, a digital forensic investigation model (DFIM) for specific applications in the IoT is proposed. The DFIM model can collect, inspect, analyze, and report reasonable forensic evidence in a dedicated DF investigation of the IoT. Literature [22] proposed the definition of forensic state acquisition controller (FSAC) in response to problems such as the nonstandardization of IoT devices and lack of connectivity. It further proposes a general framework and a method for obtaining the forensic status of the Internet of Things (FSIoT).

In 2018, Maxim Chernyshev et al. published the first journal literature review on IoT forensics [23]. The author briefly reviewed the development of digital forensics models in the IoT environment and further discussed the open problems that exist when these digital forensics technologies are applied to Internet of Things devices. Literature [24] proposes a forensic investigation framework that uses public digital ledgers to find criminal facts based on IoT systems. By collecting the interactions occurring between various IoT entities as evidence, it securely stores them in public, distributed, and decentralized blockchain networks. Literature [25] studies the mobility in the Internet of Things at crime scenes and discusses data identification and classification methods from the Internet of Things to find the best evidence. The tools and techniques for identifying and locating IoT devices are proposed. Based on the frequency and interaction mapping between devices, the recent concept of "digital footprint" was developed in the criminal field. Literature [26] proposed a blockchain-based IoT Forensics Framework (BIFF) for IoT security issues, which records events throughout the life cycle of digital evidence in a transparent, traceable, and identity privacy protection manner. Literature [27] discussed the complexity of forensics brought about by the Internet of Everything (IoE) era and further, analyzed the actual digital forensics process and the challenges that arise, and even the difficulties of the IoT forensics standards. Literature [28] studies new security issues from the perspective of cloud forensics, which mainly focuses on solving the security risks caused by customer data after customers stop using cloud services. A framework is proposed to solve the security problem of reconstructing customer data after using cloud services to delete or stop customer data.

In 2019, Francesco Servida et al. published an overview on the digital traces of IoT devices [29]. The author considers that the massive increase in IoT devices lacks existing digital forensics tools and methods and the corresponding security and privacy issues. Aiming at the application of IoT in the field of smart homes, the opportunities and challenges of IoT forensics are discussed. Literature [30] considers the security issues of cloud forensics under fog computing and points out that archiving network traffic will become the basis for key tasks such as fog computing forensics, monitoring, and troubleshooting. A new system architecture is further proposed to subtly bridge trusted hardware and searchable encryption to build a trusted, encrypted but queryable network traffic file for fog-assisted IoT applications. Literature [31] proposed a forensic analysis model. This model can acquire and analyze various Internet of things devices and serve forensic work. Taking forensic artifacts retrieved by the popular Amazon Echo as an example, the author demonstrates how to use the proposed model to guide the forensic analysis process of IoT devices. Literature [32] proposes an automatic knowledge-sharing forensics platform, which can automatically suggest a forensic mode from case data.

In 2020, Jianwei Hou et al. published a review of forensics on the Internet of Things in the top international journal IEEE Internet of Things Journal, giving a comprehensive overview of IoTF [33]. Stoyanova et al. published a review of the Internet of Things forensics in the top international journal IEEE Communications Surveys & Tutorials [34]. The emergence of these two top journal review papers means that the academic community is paying more and more attention to IoTF. They systematically review the development of IoTF in the past 10 years and summarize the classic forensic models and forensic methods. They discuss in detail the key issues that have been resolved and unresolved in the forensics process, especially the applicability of technology and legal boundary issues, as well as data security and privacy protection issues that will be faced in the future, so as to point out scientific research directions for latecomers.

4. Blockchain Technology

4.1. The Development of Blockchain. In 2008, Nakamoto [35] creatively proposed the framework of blockchain technology and proposed an idea of using Bitcoin as a decentralized digital currency. Soon, Bitcoin theory was put into practice, and this digital currency system without third-party guarantees came into being. In 2013, Buterin [36] inherited and developed the Bitcoin system, proposed the concept of Ethereum, and integrated the programmable features of smart contracts. Accordingly, the combination of the decentralization of blockchain and the programmable features of smart contracts has enabled the rapid development of the next-generation digital currency system, and a large number of virtual digital currencies such as Tether and Dogecoin have emerged. The application of blockchain also covers all aspects of people's lives. As shown in Figure 4, the blockchain architecture is a combination of a series of decentralization, trusted computing, and privacy protection algorithms.

4.2. Blockchain Data Structure. Blockchain is a distributed system, and its block structure determines the storage form of transaction information. The Merkle tree of chain structure is used to organize and manage transaction data which plays the function of connecting blocks. The data structure of blockchain transactions describes the transaction forms of Bitcoin and Ethereum and the characteristics of the generation of transaction addresses. The storage method of transaction data analyzes the design basis and development trend of the underlying data structure of the blockchain from a macroperspective. The blockchain data block structure is shown in Figure 5

4.3. Blockchain Chain Structure. Blockchain is a distributed database that links each block in order of generation time. As seen in Figure 5, the Prev-block Hash field is used to store the hash value of the previous block. All blocks are linked together in the order of generation with the Prev-block Hash field as the hash pointer. The chain structure of the above blocks forms a blockchain list, that is, a complete ledger.

The relationship between adjacent blocks in the blockchain structure is shown in Figure 6. According to the "Merkle-root" field and "Prev-block Hash" field in the block header, it can be verified by hash operation whether it has been tampered with. Relying on the Prev-block Hash field, all blocks are linked according to the creation time. If any of the blocks is tampered with, it will cause the hash value of all blocks generated afterward to change in a chain. Using the verifiability feature of the chain structure, when a node downloads certain blocks or the entire block from an untrusted node, the correctness of each block can be verified through a hash operation.

4.4. Blockchain Consensus Mechanism. The consensus mechanism is the core of decentralized trust in distributed systems. It establishes a set of mutually untrusted preset rules to realize the cooperation between nodes, which finally achieves the consistency of the data of different nodes.

Blockchain is essentially a distributed ledger record database. Therefore, the consensus mechanism in the blockchain must not only reflect the basic requirements of a distributed system but also consider the security issues of the blockchain, specifically for transaction records, the need to solve Byzantine fault tolerance, and possible malicious nodes to tamper with data. In general, the consensus mechanism in the blockchain is more targeted, and the consensus mechanism that meets different operational requirements can be selected according to different blockchain application scenarios.

Since Lamport et al. [37] put forward the "Byzantine Generals Problem" in 1982, a large amount of research on consensus algorithms has focused on theoretical discussions. But since Bitcoin entered people's sight in 2008, various consensus mechanisms have begun to move from theory to practice. With the iteration of Bitcoin itself and the development of the Ethereum platform, blockchain-based applications such as smart contracts and hyperledgers are becoming more and more abundant. Existing consensus algorithms have been improved in practice. At the same time, with the continuous emergence of new application scenarios, consensus mechanisms that meet corresponding requirements have been applied one after another.

Next, we talk about the current representative consensus mechanism in the blockchain. Table 3 compares the main characteristics of each algorithm.

5. Design of IoT Forensics System Based on Blockchain

5.1. Alliance Structure. The overall architecture is shown in Figure 7, including the client side and the server side.

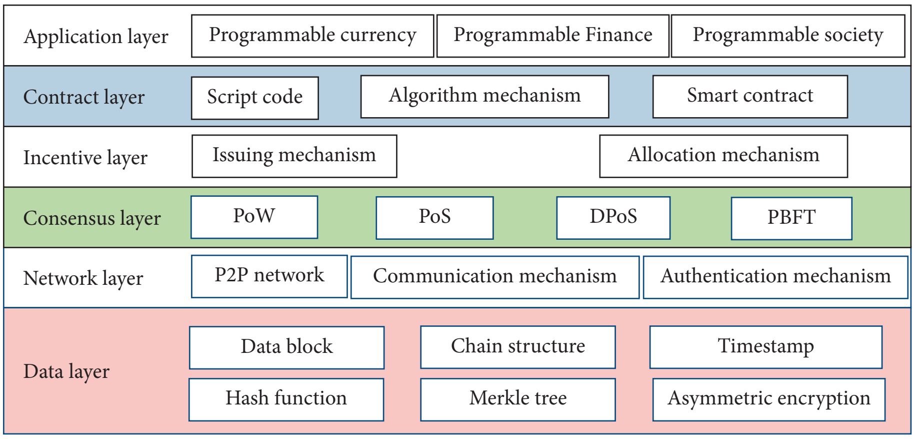

Figure 4: Blockchain infrastructure.

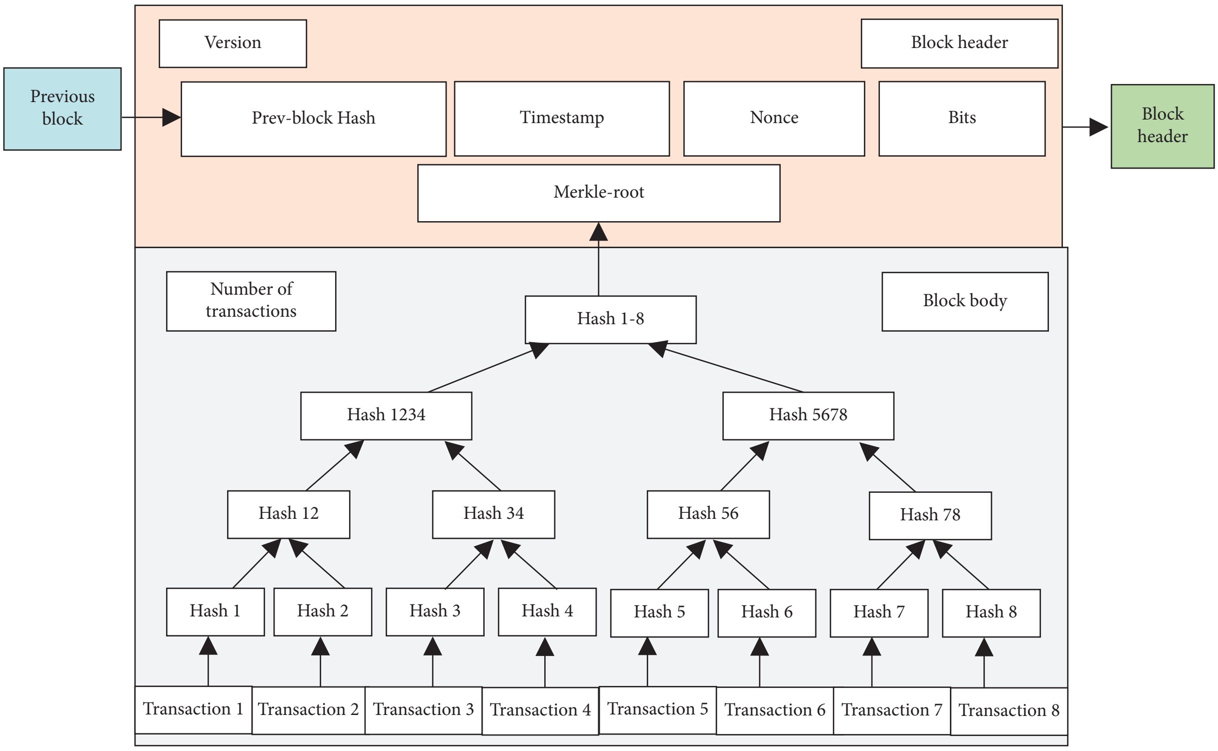

Figure 5: Blockchain data block structure.

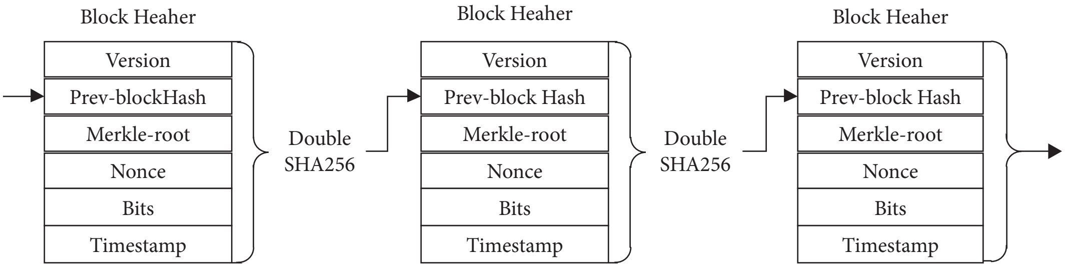

Figure 6: The relationship between adjacent blocks.

Table 3: Comparison of PoW, PoS, DpoS, and PBFT consensus mechanisms.

Parameter	PoW [38]	PoS [39]	DPoS [40]	PBFT [41]
Degree of centralization	Fully decentralized	Fully decentralized	Partially decentralized	Partially decentralized
Node access license	Not needed	Not needed	Not needed	Needed
Number of access nodes	Unlimited	Unlimited	Unlimited	Limited
Block time	Longer	Longer	Shorter	Shorter
Main resource occupation	Computing power	Equity, token	Equity, token	Bandwidth
Application scenario	Public chain	Public chain	Public chain	Alliance chain
Whether to fork	Easy to fork	Easy to fork	Not easy to fork	No fork
Final consistency	No finality	No finality	No finality	Finality
Security guarantee	More than 1/2 of computing power is credible	More than 1/2 stake is credible	More than 1/2 of equity is credible	More than 2/3 of nodes are trusted

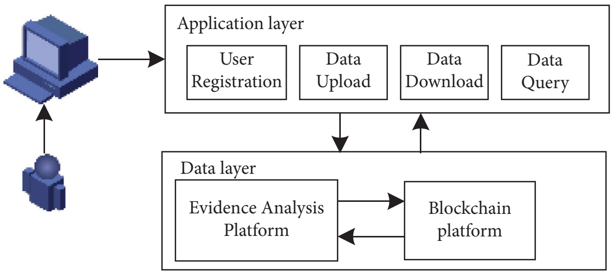

Figure 7: Blockchain-based IoT forensics overall architecture.

The overall architecture of blockchain-based IoT forensics is shown in Figure 8. In the Internet of Things environment, IoT terminals, and IoT convergence devices, regulatory agencies, judicial departments, and insurance companies form a consortium chain. Among them, IoT terminals, judicial departments, and insurance companies are light nodes, and each block header information is stored. All IoT convergence devices and regulatory departments in the jurisdiction are full nodes that are responsible for full chain storage and new block entry into the chain.

(1) IoT terminal: includes all IoT-based terminal devices, which are the most primitive generators of massive data. Equipment manufacturers regularly upload the generated data to the cloud through industry standards or corporate standards and finally upload the data to the chain through the alliance chain architecture.

(2) IoT centralized devices: usually smart switches, smart routers, and other devices with data concentration functions. These centralized devices are responsible for packaging and verifying the first-hand data, and its importance is self-evident. Relevant industry standards and regulatory measures must be promulgated first. In most cases, some cheap IoT device manufacturers have not built an enterprise cloud and will not upload data. Instead, they choose to upload data to IoT centralized devices on a regular basis.

(3) Regulatory department: it is composed of IoT enterprise representatives and industry alliances. It is mainly responsible for formulating industry standards, building an IoT forensics architecture based on the alliance chain, and guiding IoT companies to standardize data upload. When a dispute occurs or a case requires forensics and appraisal, IoT forensics shall be collected, and an appraisal report shall be issued.

(4) Judicial department: it is composed of law enforcement agencies (police and court), which can inquire and analyze the evidence stored in disputed entities in the chain and make judgments on liability and provide evidence to the insurance company to facilitate the insurance company to pay compensation.

(5) Insurance company: inquire about evidence or accept relevant evidence provided by the judicial department to decide the compensation plan alliance chain.

The IoT forensics system using the above alliance chain architecture can ensure that data is stored and obtained as safely and reliably as possible. On the one hand, the data from the Internet of Things can be directly connected to the chain, or it can be connected to the chain through an IoT centralized device. On the other hand, the supervisory departments on the chain give full play to their supervisory advantages to guide judicial departments and insurance companies to process data on the chain fairly and impartially.

5.2. IoT Forensics Model Based on Alliance Chain. Based on the overall framework of IoT forensics proposed in the previous section, it is further refined, and an IoT forensics model based on the alliance chain is proposed. As shown in Figure 9, the IoT forensics model includes 6 main modules:

(1) Data provider: it specifically refers to IoT terminal equipment. Through the device that senses and collects surrounding environment data, it sends the data upload transaction form, and after identity authentication, it provides data to the alliance chain. The data is stored in the distributed storage system in ciphertext form, and the data summary is stored in the blockchain network.

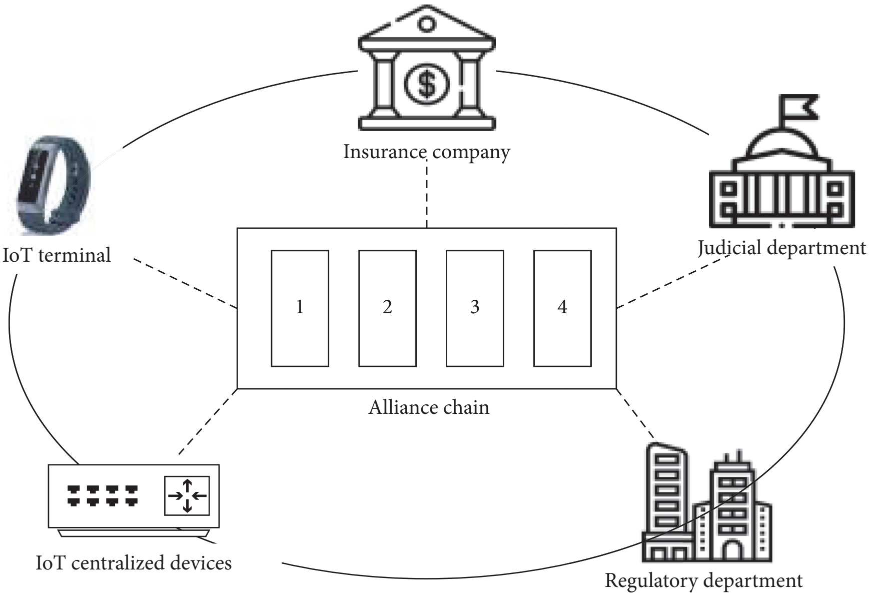

Figure 8: IoT forensics alliance architecture.

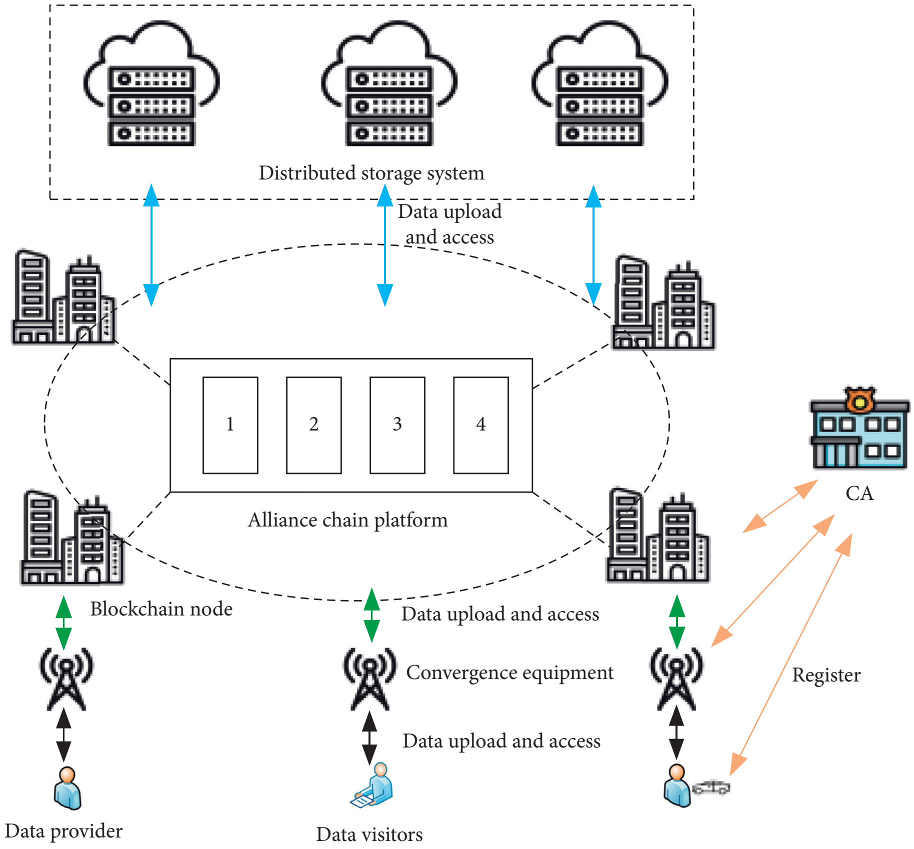

Figure 9: IoT forensics model based on alliance chain.

(2) Data visitors: they mainly include ordinary users, judicial departments, regulatory authorities, and insurance companies. Request corresponding data from the alliance chain by sending data access transactions. After identity authentication and access authority verification, the required data is obtained from the alliance chain.

(3) Convergence equipment: it is responsible for receiving data from the data provider and verifying the identity of the data requester and the integrity of the data packet.

(4) Alliance chain platform: iIt is built and maintained by a group of blockchain nodes to record data upload and data access in the consortium chain. The members of the alliance chain include IoT terminals, IoT convergence devices, regulatory agencies, judicial departments, and insurance companies. The purpose is to solve the problem of protection of the integrity and verifiability of evidence in the platform.

(5) Distributed storage system: it is used to store encrypted data packets in the blockchain network.

(6) CA: iInitialize the entire IoT alliance blockchain network, register each entity, and then keep it offline.

5.3. Data Provider's Perspective-Evidence Flowchart. This section discusses the IoT storage process based on the alliance chain from the perspective of the data provider, as shown in Figure 10.

(1) Login/Registration: before completing the deposit, the data provider (the deposit certificate user node) needs to complete the login/registration procedure with the CA to confirm the identity information and corresponding permissions. At the same time, the performance information of other user nodes is obtained, and reference data is obtained for subsequent data fragment storage.

(2) Electronic data fragmentation: the system uses a redundant fragmentation algorithm to fragment the uploaded electronic data And then select a number of nodes with the best performance based on the node performance information obtained previously to store the fragmented data of the system.

(3) Upload certificate files: users upload the files that need to be certificated and write the key information of the files into the contract file category. In this way, the corresponding mapping relationship between users and data is established.

(4) Verification of deposit documents: the system reads the relevant storage information of electronic data from the contract, obtain the location of the electronic data storage by storing the information and downloading the electronic data fragments, and restore the data and compare the file hash value to verify the integrity of the electronic data.

(5) Offline: the user logs out and ends this deposit operation.

5.4. Data Visitor's Perspective-Evidence Flowchart. This section discusses the IoT forensics process based on the alliance chain from the perspective of data visitors, as shown in Figure 11.

(1) Preparation: the forensics personnel needs to sort out the briefcase of the case before performing the verification operation, confirm the specific IoT forensics scenarios, and evaluate the potential forensic objects on-site and the evidence that needs to be collected.

(2) Initialization: the main event detection, first response, and investigation preparation aspects of the forensic initialization work. It is mainly to respond to the on-site evidence collection environment in a timely manner, and it is best to obtain on-site evidence as quickly as possible.

(3) Investigation: during the investigation phase, forensics personnel obtains, tests, analyzes, and screens evidence and tries to reconstruct the incident using the obtained evidence. Based on the refactored matter, the question of investigation and evidence collection is reversed, and relevant evidence for evidence collection is supplemented.

(4) On-chain interaction: in on-site investigation and evidence collection, through hash calculations and electronic signatures, the first-hand forensic data can be stored on the chain for the first time through the network, thereby curing it into data that cannot be tampered with. At the same time, it is also necessary to call the existing information on the chain for verification when collecting evidence on the spot, and the use of the alliance chain will be more flexible.

(5) Report: at the final stage of the forensic collection, a forensic report is issued. Through feedback from relevant units, confirm whether to return to the investigation stage to supplement the secondary evidence collection work.

5.5. Examples of IoT Forensics. The IoT has been integrated into every aspect of our lives, which makes the examples of IoT forensics everywhere. With the innovation of cloud computing, big data, artificial intelligence, and other technical means, UAV has led the current trend of smart consumption due to their high technological content and fashion sense. The UAV has more and more applications in daily consumption scenarios such as entertainment and life, which makes the demand for drone forensics more and more urgent.

This section takes DJI Mavic 2 pro as the experimental object to extract and analyze its data and try to give everyone a preliminary understanding of IoT forensics. The Mavic 2 pro series have a built-in SD card and are assisted by the APP installed on the mobile phone, which makes the mobile phone retain a large amount of original data of the UAV. This experiment adopts the mobile phone APP forensics method, which is also one of the most mature methods of digital data forensics.

As shown in Figure 12, the red curve represents the flight path of the UAV, and the blue curve represents the movement path of the UAV controller. In addition, the detouring and stagnant behavior during UAV flights can also be reflected by repeating the lines and adding groups. In

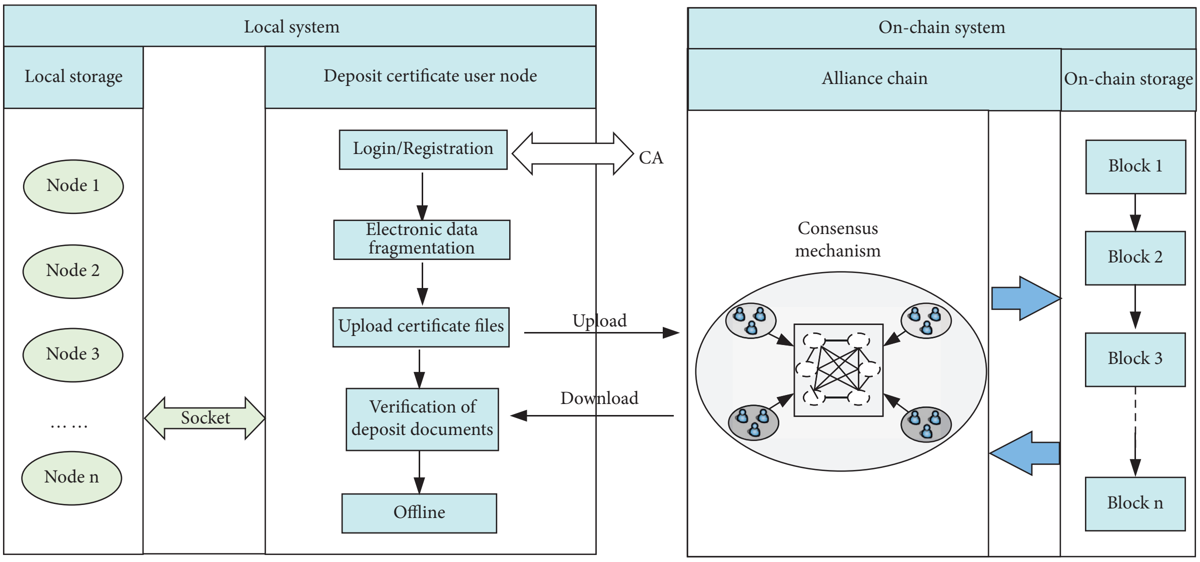

Figure 10: Data Provider's perspective-evidence flow chart.

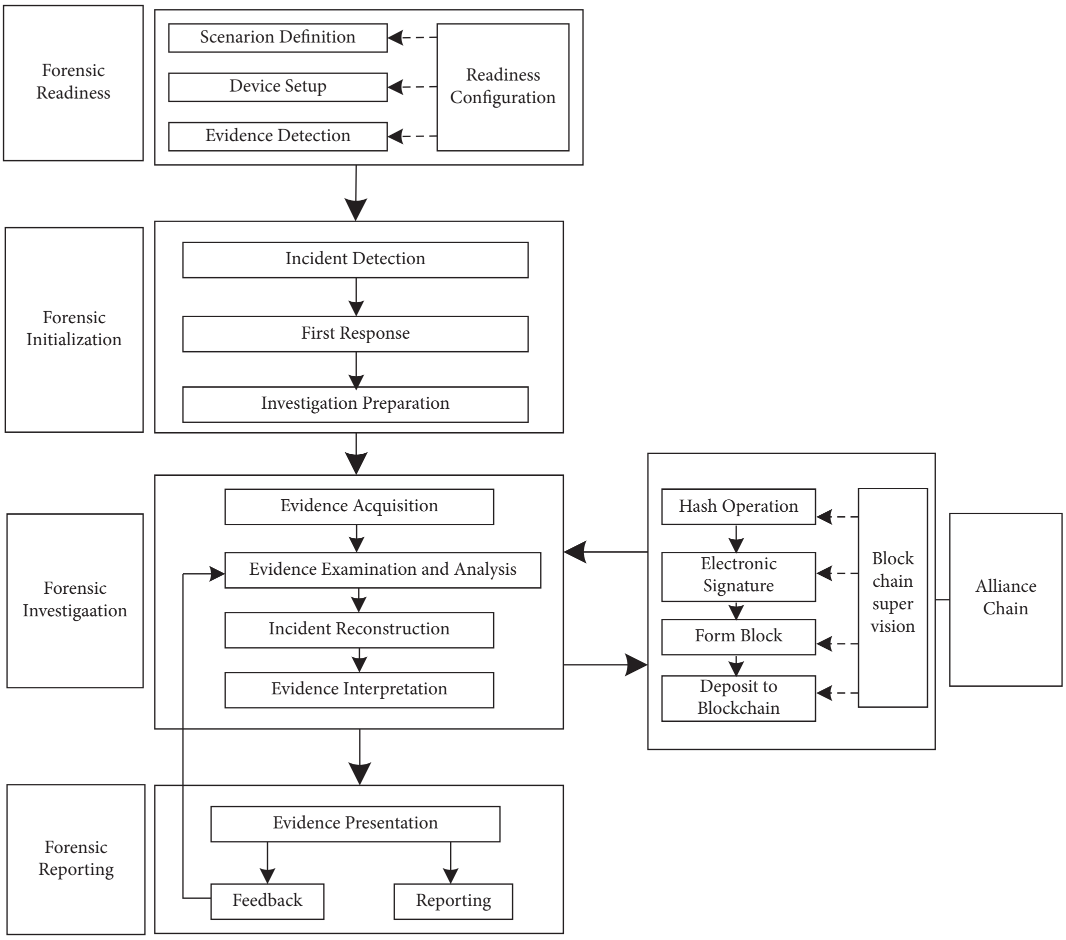

Figure 11: Data visitor's perspective-evidence flowchart.

addition to analyzing the flight path of the UAV, the photos and videos taken by the UAV are also important evidence, which involves traditional digital forensics, and we do not do much research.

Another important feature of the UAV is the lack of battery life, so the power management of the UAV is an important research direction. As seen in Figure 13, the voltage of the UAV and the remaining battery power can be analyzed. We found

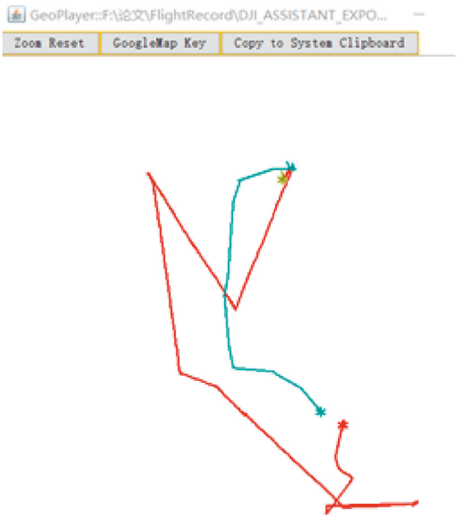

FIGURE 12: UAV flight path.

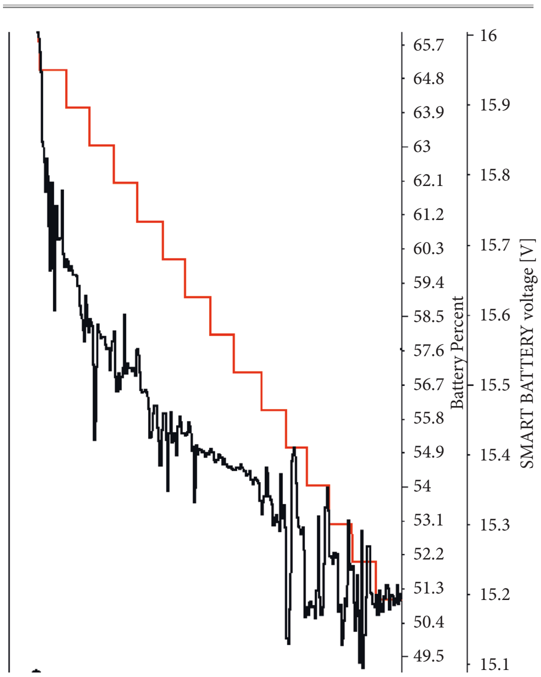

FIGURE 13: UAV voltage and remaining battery power.

that the battery power of the drone is 65% (red line) during flight, and as the power usage of the drone declines in steps, the battery voltage also peaks at around 16V due to the drone taking off. Then the battery voltage drops slowly and fluctuates slightly. By analyzing the battery and charge of the UAV, it is possible to confirm the behavior of the UAV at the time, which is valuable for further forensic analysis.

6. Conclusions

This article conducts research on IoT forensics and compares its differences with traditional DF. We further sort out the research results of IoT forensics in recent years. Through the research of blockchain technology, it is introduced into the IoT forensics framework. An IoT storage and forensics system based on the alliance chain is proposed. Subsequent research will consider privacy issues in the forensics process.

Data Availability

The experimental data used t support the findings of the study can be obtained from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

An earlier version of this research has been presented as a conference publication at International Conference on Artificial Intelligence and Security (ICAIS) [14]. It has been supported by the National Natural Science Foundation of China (Grant no. 61802155), The Major Project Contract for Natural Science Research of Jiangsu Colleges and Universities (Grant no. 20KJA520004), Open project of the National and Local Joint Engineering Laboratory of Radio Frequency Integration and Micro-assembly Technology (Grant no. KFJJ20200201), 2021 Jiangsu Police Officer Academy Scientific Research Project: Research on D2D Cache Network Resource Optimization Based on Edge Computing Technology (2021SJYZK01), and High-Llevel Introduction of Talent Scientific Research Start-up Fund of Jiangsu Police Institute (JSPI19GKZL407).

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 Things Journal*, vol. 8, 2021.

[4] N. Miloslavskaya and A. Tolstoy, “Internet of Things: 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 digital

forensics 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 Third 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 blockchain-based 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 Blockchain-Based Internet of Things 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 privacy-aware IoT-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, "IoT forensic," 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. Thing, "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 Things 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 Things 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 Things 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 Things 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 Things (IoT) Forensics: Challenges, Approaches and Open Issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[35] S. Nakamoto, "Bitcoin:A peer-to-peer electronic cash system," 2009, https://bitcoin.org/bitcoin.pdf.

[36] V. Buterin, "next-generation smart contract and decentralized application platform(white paper)," 2019, https://github.com/ethereum/wiki/wiki/White-Paper.

[37] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[38] B. Adam, “The Hashcash Proof-Of-Work function(draft),” 2003, http://www.hashcash.org/papers/draft-hashcash.txt.

[39] D. Larimer, “Transactions as Proof-Of-Stake,” 2013, http://7fvhfe.com1.z0.glb.clouddn.com/wp-content/uploads/2014/01/TransactionsAsProofOfStake10.pdf.

[40] A. Bisola, “Delegated Proof-Of-Stake (DPoS) explained,” 2018, https://www.mycryptopedia.com/delegated-proof-stake-dpos-explained/.

[41] J. Fan, L.-T. Yi, and J.-W. Shu, “Research on the technologies of byzantine system,” *Journal of Software*, vol. 24, no. 6, pp. 1346–1360, 2014.