Chapter 7
Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger

Haider Al-Khateeb, Gregory Epiphaniou, and Herbert Daly

Abstract Blockchain technology can be incorporated into new systems to facilitate modern Digital Forensics and Incident Response (DFIR). For example, it is widely acknowledged that the Internet-of-Things (IoT) has introduced complexity to the cyberspace, however, incident responders should also realise the advantages presented by these new "Digital Witnesses" (DW) to support their investigation. Logs generated by IoT devices can help in the process of event reconstruction, but their integrity -and therefore admissibility- can be achieved only if a Chain-of-Custody (CoC) is maintained within the wider context of an on-going digital investigation. Likewise, the transition to electronic documentation improves data availability, legibility, the utility of notes, and therefore enhances the communication between stakeholders. However, without a proof of validity, these data could be falsified. For example, in an application area such as eHealth, there is a requirement to maintain various existing (and new) rules and regulations concerning authorship, auditing, and the integrity of medical records. Lacking data control could lead to system abuse, fraud and severe compromise of service quality. These concerns can be resolved by implementing an online CoC. In this paper, we discuss the value and means of utilising Blockchain in modern systems to support DFIR. we demonstrate the value of Blockchain to improve the implementation of Digital Forensic Models and discuss why law enforcement and incident responders need to understand Blockchain technology. Furthermore, the admissibility of a Digital Evidence to a Court of Law requires chronological documentation. Hence, we discuss how the CoC can be sustained based on a distributed ledger. Finally, we provide a practical scenario related to eHealth to demonstrate the value of this approach to introduce forensic readiness to computer systems and enable better Police interventions.

H. Al-Khateeb (✉) · G. Epiphaniou · H. Daly
University of Wolverhampton, Wolverhampton, UK
e-mail: H.Al-Khateeb@wlv.ac.uk

H. Jahankhani et al. (eds.), *Blockchain and Clinical Trial*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-11289-9_7

Keywords Digital investigation · Forensic readiness · Incident response · Digital witness · Decentralised computing · Liability attribution · eHealth · Data integrity · Digital evidence

7.1 Introduction

Digital Forensics has disseminated to cover the wide variety of technologies we utilise, in an era where connected devices (IoT) are forecasted to be around 30 Billion (Navarro-Ortiz et al. 2018). Digital Forensics is a prominent and inevitable part of an Incident Response plan covering electronic data and an established skill area in the cyber security industry. Examples of legal recognition in the United States goes back to 2006 when courts adopted new rules for civil procedures to acknowledge digital information as an acceptable form of evidence and implemented a mandatory system, namely electronic discovery (eDiscovery) to establish the grounds for this new branch of forensic science (Navarro-Ortiz et al. 2018). In present days, one approach in which the National Cyber Security Centre (NCSC) in the UK addresses the vision of the UK Cyber Security Strategy 2016–21, “the UK is secure and resilient to cyber threats, prosperous and confident in the digital world”, is by certifying Bachelor and Master’s degrees where Digital Forensics is a clearly defined path alongside few other well-established titles such as cybersecurity, information security, and computer network and Internet security.

The main purpose of Digital Forensics is to perform technical investigations within the boundaries of the legal system in response to criminal activities that involve electronic devices. The objective is to support or reject a hypothesis related to a criminal or civil case. Disputes between commercial parties could also be the reason for performing eDiscovery within this context. Forensically sound tools (sound; vetted and tested thoroughly) are utilised by trained investigators to collect, analyse and reconstruct events and actions to help to explain what happened in support of a prosecution (Daryabar et al. 2017). Technical investigators are referred to as Expert Witnesses, and they become responsible to produce a conclusion that is admissible to a Court of Law.

The scope of digital investigations continues to increase. Building an effective team requires specialist skills in areas such as computer and mobile phones, onsite (crime scene) investigations, call data records, search orders, forensic readiness planning, data recovery, and audio-visual forensics. Non-electronic data is within the scope as well considering the highly integrated cyber-physical ecosystem we interact with. For instance, a digital currency such as Bitcoin can be saved offline as part of a paper-wallet. This approach is attractive for users who aren’t tech-savvy, to enable offline money exchange, or to keep Bitcoin addresses safe against online attacks on the long-term. Therefore, a forensic investigator would be expected to seize this offline storage medium in cases associated with money laundering or illegal dark web trading. A Bitcoin paper-wallet is usually designed with elements of physical security; a folded design to resist shoulder-surfing. Additionally, tamper-resistant measures such as anti-candling hologram stickers are used which shows that offline analysis techniques could become one of the required skillsets for the team. Another example to demonstrate the extended scope of modern digital investigations to involve body scanning is the emerging practice of microchip implants. In 2018, thousands of people in Sweden have inserted microchips into their hands for identity check; to access their office at work, gym, and pass through train gates (Pollitt 2010).

This paper discusses the utilisation of Blockchain for modern DFIR. The need for a tamper-proof series of timestamps could be traced back to the 1990s while the first conceptualisation of the technology was described in a white paper authored by Satoshi Nakamoto (a fictional name) in 2008 (Nakamoto 2008) to enable distributed Bitcoin transactions. The Blockchain is formed of a basic list of records, namely blocks, which are linked using cryptographic algorithms. The solid connection and continuity of blocks prevent the modification of existing data blocks and any written content will, therefore, be verifiable and permanently accessible. This has triggered a lot of interest from various industries such as banking and energy, while other proposals were presented to support governance models (Mengelkamp et al. 2018; Cocco et al. 2017). Consortiums have been established and private research labs opened to investigate potential models that could help to cut the middle-man (which is cost-effective) and automate processes for businesses back-end systems (Johng et al. 2018). Furthermore, the distributed nature of the technology removes any single-point-of-failure and provides the mean to hold participating parties accountable for their records because each recorded transaction will be witnessed by all connected nodes and only an enormous amount of computing power can override their data. Possible in theory but non-practical; attacking the network becomes harder when more self-motivated devices become part of the distributed system. The need for provenance tracking goes beyond the financial and supply chain markets as it is also a very critical requirement for forensic investigations. Tracking the origin and movement of case-related data (e.g. seized items) is challenging as it is subject to human error, theft and counterfeiting. A recent example from Iceland showed that poor work practices have been reported as the reason for the disappearance and untreacability of seized assets following a Police raid (Daryabar et al. 2017).

Records on the Blockchain are virtual and representatives of any seized item, therefore suitable to support the creation of a CoC compared to a paper-based solution that can be destroyed or a central system that can be vulnerable to Denial-of-Service (DoS) and less resistance to integrity attacks. To elaborate, once a physical or electronic item is seized, a virtual token is created to act as a certificate of authenticity for that item at that specific time. Thereafter, a new virtual token is created to openly evident changes to that item during transport or alteration. Other metadata can also be supported which allows the CoC to include other useful information.

In the remaining part of this chapter, the reason why law enforcement investigators should understand and utilise Blockchain technology is discussed in Sect. 7.2, how Blockchain technology can improve the implementation of digital investigation models is discussed in Sect. 7.3, and how a Chain-of-Custody (CoC) can be maintained with Blockchain is demonstrated in Sect. 7.4. Then, Sect. 7.5 presents a case study related to eHealth to demonstrate the value of this approach to introduce forensic readiness to computer systems and enable better Police interventions. Sect. 7.6 discusses Digital Witnesses (DW). Finally, we conclude our chapter in Sect. 7.7.

7.2 Why Police Digital Investigators Need to Understand Blockchain Technology

7.2.1 To Maintain Compliance with Digital Investigation Principles

Law enforcement agencies perform digital investigations to reconstruct events from the past in support of on-going cases. However, not all investigations can be prosecuted due to reasons not limited to the nature of the incident but also the validity and integrity of the investigation process itself, this is where Blockchain technology becomes useful. The technology can help compliance with guidelines. In the US, the Department of Homeland Security, US Secret Service has published Best Practices for Seizing Electronic Evidence as a pocket guide for first responders (U.S. Department of Homeland Security – United States Secret Service 2015). In the UK, the Association of Chief Police Officers (ACPO) has agreed to a set of guidelines to be adopted by Police Forces in England, Wales & North Ireland. Non-compliance can be a reason to invalidate the integrity of the investigation. The principles listed in the ACPO Good Practice Guide for Digital Evidence (Williams 2012) are:

Principle 1: “No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court”.

Principle 2: “In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions”.

Principle 3: “An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result”.

Principle 4: “The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to”.

These principles, especially Principle 3, is clearly enforcing a verifiable audit trail on the investigation process. Blockchain-based Digital Investigation Models can help to achieve that as discussed in Sects. 7.3 and 7.4.

7.2.2 To Facilitate Multijurisdictional Investigations

The cyberspace is cross borders. Therefore, multijurisdictional investigations are routinely pursued by law enforcement agencies around the world. As such, there are various frameworks and models addressing miscellaneous technologies (e.g. IoT), case studies, crime scene scenarios and local laws. This complexity is an obstacle as it is resource consuming and introduces many legal challenges. Additionally, there are International Organization for Standardization (ISO) standards such as the ISO/IEC 27037 to comply with as well. It provides guidelines for the identification, collection, acquisition and preservation of Digital Evidence while another standard namely the ISO/IEC 27043 provides guidelines based on idealised models for common incident investigation principles and processes. A key enabler for multijurisdictional investigations is the utilisation of a collaborative environment and a permission-based model to share evidence. Hence, the possible value of a Permissioned Distributed Ledger System (Permissioned Blockchain) for law enforcement.

7.2.3 To Have More Witnesses

While some crimes are reported or supported by a witness accepted by a Court of Law, others are hearsay and might not be as valuable to support a prosecution unless we have means to trace records back to their originator. In the cyberspace, the concept of DW has been introduced. Despite many challenges and complexities introduced by the IoT paradigm, it has also empowered digital investigations with new DWs. This can be an IoT device capable of preserving and sharing data (Digital Evidence) with other connected devices or the cloud. Collaboration between IoT devices is at the core of this approach and Blockchain is a key facilitator to establish a trusted CoC.

Accepting devices to act as a DW requires specific properties. For example, anti-tampering behaviour, binding credentials, binding delegation, and accepted procedures as discussed in (Nieto et al. 2016). The "anti-tampering behaviour" property means that an IoT device should have a solid security feature such as an embedded Trusted Computing Hardware to periodically verify its integrity. The device should invalidate its own eligibility to be a DW in cases of malfunctioning or failures of integrity checks. Blockchain-based models are being developed to trace the status of these devices and securely record relevant values as part of a digital CoC.

7.2.4 To Support Victims with Blockchain-Based Forensic-Enabled Devices

Victims of cybercrime are usually keen to construct and maintain Digital Evidence to support their assertion. They will, therefore, be interested in forensic-enabled solutions as part of their cyber safety. For instance, victims of cyberstalking (al-Khateeb et al. 2017) cannot predict the time or means they will be targeted and would adopt forensic-enabled software and hardware to preserve Digital Evidence. Captured information can be used to report and escalate the incident with the Police and increase the chances of acquiring evidence that is admissible to a Court of Law. Furthermore, victims should not have to be tech-savvy while digital investigators are expected to utilise the opportunity presented by Blockchain forensic-enabled devices to support the case towards suitable prosecution.

7.2.5 To Investigate Technology Misuse

Digital investigations cover any electronic data including the many current and future Blockchain-based implementations. Cryptocurrency (e.g. Bitcoin) transactions are recorded on a Blockchain making the technology a topic of interest because cryptocurrencies are widely used in the Dark Web, subject to money laundering, tax evasion, and price manipulation. In 2018, the Federal Bureau of Investigation (FBI) reportedly "has 130 cases tied to cryptocurrencies", according to Supervisory Special Agent Kyle Armstrong, speaking at the Crypto Evolved conference in New York.

7.2.6 To Develop New Solutions in Response to Emerging Digital Forensics Challenges

Digital investigators work in the field with hands-on experience. They are in a good position to provide the required feedback based on existing challenges. A good understanding of what technology can offer helps practitioners to contribute towards deploying new solutions. For example, the following classifies the widely reported challenges facing digital investigations:

Technical Challenges Represented by the evolvement of new devices (e.g. IoT) to address, new models (e.g. Cloud Computing) to understand and prepare for, and increased volume of data to preserve and analyse (e.g. Big Data).

Legal, Regulatory and Procedural Challenges We need to develop the means to facilitate national and cross borders investigations while adhering to local laws.

Likewise, incident response within a specific company is governed by corporate policy and procedures. Moreover, many standards and models are introduced while compliance is complex and varies between stakeholders.

Social Challenges For example, problems that victims of cybercrime face when considering a voluntary hand over of their personal digital devices to preserve Digital Evidence. This has a clear impact on their privacy as well as losing access to their own personal assets.

7.3 How Blockchain Technology Can Improve the Deployment of Digital Investigation Models

7.3.1 Introducing Digital Investigation Models

There are several published investigation models and they all attempt to elaborate on the steps to be taken by the forensic team. For example, to define the principles, tasks and responsibilities to maintain the integrity of the preserved evidence. They aim to achieve this without contradicting any local jurisdictional laws and regulations, the team would, therefore, exercise with care to maintain compliance with the prevailing jurisdictional requirements. Digital forensics is all about the process, it is a recognised scientific methodology and should be designed to provide the ability to verify all reported conclusions (or process output). The initiation stage is usually triggered by a reported incident. In its simplest form, an investigation model could consist of: acquisition, analysis and reporting. However, the complexity of the cyberspace attracted various revisions. In an early paper (Navarro-Ortiz et al. 2018), four stages were suggested namely "acquisition", "identification", "evaluation", and "admission as evidence". In knowledge management terms, data is usually captured from a seized media within a physical context, processed for evaluation within a logical context, and finally submitted as evidence within a legal context. This model was then amended in 2001 as part of the first Digital Forensic Research Workshop (DFRWS) (Pollitt 2010) to six stages starting with an "identification" phase to detect incidents as part of proactive monitoring or auditing to trigger the forensics process. A "preservation" phase where procedures for case management are introduced to maintain the integrity of evidence collection. The "collection" phase where data is extracted from the crime scene for further processing at a consequent stage called the "examination" phase. Captured data is then "analysed" to locate and recover hidden artefacts and report any incriminating evidence. Finally, a concluded evidence statement is reported as part of a "presentation" phase.

The IT security catalogue from ISO includes standards focusing on electronic discovery (eDiscovery) namely ISO/IEC 27050-1:2016, ISO/IEC 27050-3:2017, and ISO/IEC 27050-2:2018. Overall, they aim to locate and preserve pertinent Electronically Stored Information (ESI) including data by any stakeholder involved in the investigation. The ISO/IEC 27050-1:2016 defines key concepts within seven main stages very similar to the those developed by the DFRWS model starting with “identification”, “preservation”, and “collection”. The consequent steps and their details have then been developed as: “procession”, “review”, “analysis”, and finally ESI “production”. Other relevant standards such as the ISO/IEC 27037 are also covered to describe related activities and needed interactions. ISO/IEC 27050-3:2017 provides a code of practice for eDiscovery and practical measures covering the duration of the ESI lifecycle from the initial creation to the final disposition. Finally, the ISO/IEC 27050-2:2018 supports the eDiscovery process with guidance for governance and management. While all documents are written to be used by both technical and non-technical personnel, this standard aims at senior management levels within a company including those with requirements for regulatory and industry standards. It helps to advise on how to select and maintain ownership of risks related to eDiscovery. This usually involves developing as well as implementing the required policies in order to achieve internal and external compliance.

The DFRWS framework and ISO/IEC 27050 have been designed as general-purpose frameworks for ESI, the investigators must follow up revisions aimed at coping with advancement in technology or to meet the requirements of specific case studies. For instance, (Daryabar et al. 2017) argued that tailoring of existing models is required; the study developed a domain-specific cyber forensic investigation model for higher education institutes in which a policy was incorporated to address the capabilities and nature of this environment. Another study (Ma 2018) redefined the investigation phases as “classes”, while actions within each class were defined as associated “elements”. The authors then utilised Coloured Petri Net (CPN) modelling to represent the overall process. Furthermore, discussions in this area of research went beyond introducing a comprehensive or tailored framework to introducing loop-back activities were revisions were encouraged during the digital investigation life-cycle to confirm actions and achieve better reliability (Nakamoto 2008).

7.3.2 Integrating Blockchain Technology for Digital Investigation Models

To address the question of how Blockchain technology can help to achieve the aims of existing digital investigation models, we should consider a generic framework such as the DFRWS framework and the ISO/IEC 27050 standards. Figure 7.1 demonstrates the framework while incorporating knowledge management terms (Navarro-Ortiz et al. 2018) to discuss the integration of Blockchain technology.

The “identification” phase incorporates several actions including -but not limited to- incident detection, resolving file signatures, profile detection, anomaly detection, system monitoring, complains, and audit analysis. These actions are key enablers for the forensics process because there can be no case to investigate if no

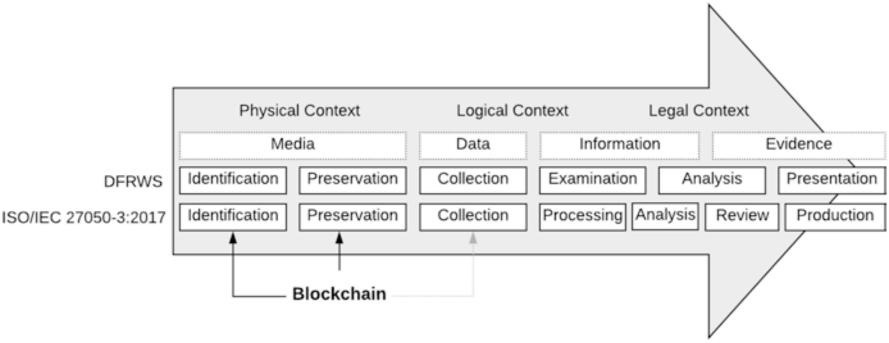

Fig. 7.1 The role of Blockchain as part of the wider digital investigation process can be realised by automating the "identification" and "preservation" phases

event was reported. While these actions seem to be contained within a physical context, at first sight, they are practically required to address all the legal requirements to satisfy a Court of Law in the case of a crime which is usually finalised during the "presentation" stage. Traditionally, this early logging of events will only be hashed during the data "preservation" phase following the creation of a forensic image, because systems -by default- are not forensic-friendly. However, Blockchain-based systems could introduce an automated implementation were all events are logged as part of a growing list of records (blocks). Each block contains a cryptographic hash of the previous block in addition to a timestamp. Hence, systems will be -by design- forensic-enabled. Both the "identification" and "preservation" phases are concerned with the media to be captured. The media in this context can contain an artefact of interest whether it is network traffic, volatile memory, physical storage or other forms of electronic data.

The "preservation" phase traditionally covers forensic imaging to create an identical electronic copy of the original, this image is then hashed. This is when a CoC is introduced and maintained per the ACPO guidelines. However, the introduction of Blockchain at an earlier phase provides opportunities such as:

Data Availability Records can be backed up and stored in several places, their integrity can always be verified separately -when needed- relying on the Blockchain.

Continuous Fraud Detection and Forensic Readiness The Blockchain can be used to automate processes, it introduces forensic readiness to systems, and several copies of the Blockchain exist in remote locations which reduced the risk of deletion.

Efficiency The maintenance of data integrity will not be time-consuming for the investigators.

Reliability Since records are already hashed as part of a trust-worthy automated process establishing a chain of blocks, there will be no risk to the investigation related to the miscalculation of hashes. Traditionally, hashes are calculated several times when the crime scene is inspected.

Therefore, the "collection" phase in which forensically sound software and hardware tools are utilised can start immediately. As part of this phase, case-relevant artefacts and data remnants are extracted in preparation for the additional examination. Hence, the value of integrating Blockchain technology in digital investigation models can be seen in the automation of the "identification" and "preservation" phases, and to a degree, in the "collection" phase if the system is designed to store some of its critical data (e.g. identifiers) in the Blockchain directly. While Blockchain technology is not meant for data storage due to computational complexities, it is theoretically possible to store data on a Blockchain. These early phases in the investigation model are the core part to facilitate evidence presentation within the expected legal requirement which leads to the final legally-binding case decision.

To integrate the technology, one of the three high-level types of Blockchain implementations should be considered. A public Blockchain is shared in the wild (Internet) with no access restriction which means that any participant can send a transaction or act as a validator on a voluntary basis. The benefit of this approach (as seen with Bitcoin and Ethereum) is the existing evidence of popularity due to the included economic incentive given to volunteering participants. Another benefit is the devices ability to join and exit at any given time within predefined rules, this can be useful to provide integrity checks for a wide range of IoT devices acting as DWs without requiring infrastructure cost; there is no need for the vendors to maintain data centres or pay for system and network administrators. On the other hand, private Blockchains require registration and approval, a participant must first be invited by the network administrators, but transactions are relatively faster than public Blockchain networks. The key benefit of this approach would be the ability to maintain a CoC without exposing data to the public Internet, and the ability to know the identities of all participants. A hybrid approach is also possible with a consortium Blockchain in which several companies practising control, it is therefore permissioned and semi-decentralised. With regards to Digital Forensic Models, all the three types of Blockchain implementations can contribute to the creation of a digital CoC. Cryptography can be used to secure sensitive data sent to a public Blockchain making it a feasible option. Identifying a participating device from the network is not always required because the CoC starts from the device itself (DW) and is therefore known and linked to the Blockchain, not the other way around as demonstrated in Fig. 7.2. Furthermore, as the Blockchain technology is emerging, some argues that any non-public Blockchain implementation could suffer the fate of the Intranets in the 1990s when companies built their private capabilities within their perimeters. Then, Intranets became less popular with the advent of web-based services such as the Software-as-a-Service (SaaS) products.

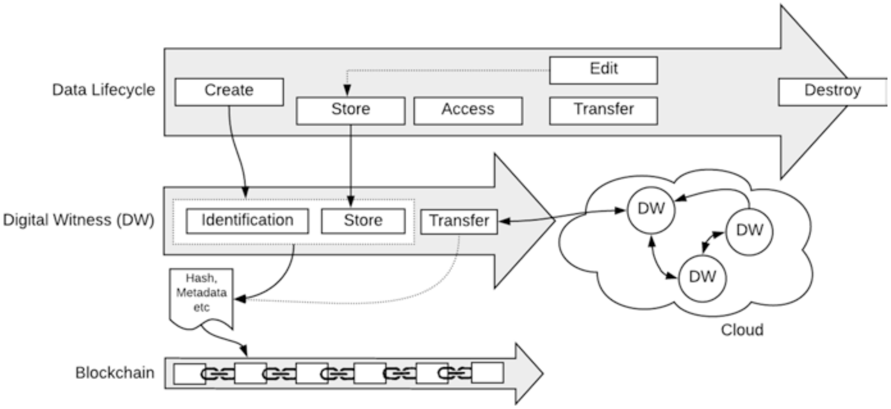

Fig. 7.2 The role of DW is to identify and preserve data. Data can be stored on the device or transferred to other devices (Hearsay DW) in the cloud. The Blockchain is utilised to initiate the Digital Chain-of-Custody (CoC) as early as when the data is created

Table 7.1 Excerpt sample worksheet from "Appendix: Resources" of the fundamental computer investigation guide for windows by microsoft corporation

Evidence description /number	Acquisition date	Acquisition location	Acquisition method	Acquired from	Acquired from (signature)	Storage location
	Transfer date	Transferred to (location)	Transfer reason	Now in custody of	Now in custody of (signature)	Storage location
Additional notes						

7.4 Towards a Blockchain-Based Digital Forensic Chain-of-Custody

Like fingerprints and DNA, the value of Digital Evidence in a crime scene. However, it is more fragile and easily lost if the investigators do not follow suitable precautions. In law, CoC documentation provides the required admissibility and proof of validity. Table 7.1 shows an excerpted sample from a worksheet designed to log the relevant details when investigating a computer, this CoC Log Documentation was developed and published by Microsoft as part of their Fundamental Computer Investigation Guide for Windows.

CoC logs vary in their design, they can be very detailed as a mean to remind investigators of all the required details to think about and write down. Others, however, are more adaptable to the real needs of the crime scene by requesting fundamental details valid for all cases while amending a space for additional notes. An example for the several questions to think about at the crime scene:

- Was the seized object intentionally hidden?
- Was the seized computer connected to a kill switch?

These questions are not valid for all scenarios but can be very critical crime scene notes and should be documented to support the investigation at a later stage. Therefore, a well-designed CoC log allows enough space and incorporates guidelines to enforce good systematic practice. A CoC within a legal context is defined as the sequence of documented actions performed during forensic investigations. This covers all the stages of the adopted investigation model from acquisition and seizure to the presentation of findings. Traditionally, the CoC is based on a paper trail. However, with the emergence of the alternative -digital- mediums the term "paper trail" could also describe other methods to maintain an audit. That said, a more inclusive term would be "audit trail". Overall, a CoC form serves the following functions:

- Identifies the evidence.
- Identifies who has handled the evidence
- Describe actions performed, or to be performed, on the evidence: control, transfer, analysis and disposition.
- Lists dates and times the evidence was handled.

The authenticity of each record in the CoC has a significant value to the investigation as it could be used to convict a suspect to a specific crime. Contamination of seized files would raise suspicions that certain events were fraudulently planted and would, therefore, disqualify the evidence. A CoC could also link a physical object (e.g. a memory disk) to an individual. In cases where the defendant claims no prior link to the seized object being investigated, the CoC is utilised by the prosecution to demonstrate that the object was in the possession of the defendant at the time of seizure. As a general role, the CoC must document every action and every evidence transfer between persons from -and as early as- evidence acquisition. It must be verifiable that no other persons could have altered -or accessed- that evidence. Therefore, to restrict access, the recommendation is to keep the number of transfers as low as possible.

The CoC is how the accountable law-enforcement officer is identified during the lifetime of the investigation. Several officers could take part due to separation of duties, hence a crime scene investigator will be named on the CoC to have the physical custody of the seized evidence, while other identifiable officers can be named afterword on succeeding transactions in chronological order. The required transactions metadata include timestamps and the signature of officers involved at each step, while examples of other metadata include the name of the law-enforcement agency, case number, date of receipt, date of report, in addition to a detailed descriptive list of related seized items with their serial numbers, make and models. Traditionally, this information is written as part of a "Bag and Tag" practice directly on the bag containing the evidence.

When the investigators are dealing with electronic evidence extracted from a live environment such as connected servers, or powered machines, the CoC plays a critical role to document actions. The known Locard exchange principle, also known as

Locard's theory, states that any contact between items will cause an exchange. In the digital realm, this translates into any contact between computers, a computer and a storage device or utilising an input device which includes moving the mouse to click on the screen. However, in the context of a live environment, there are many important artefacts residing in the computer's Physical Memory including but not limited to user credentials, running processes, DDLs, encryption keys, files, open sockets and Registry Keyes. Physical Memory is stored on RAM chips lined up in built-in notches on the motherboard. Therefore, the evidence acquisition stage is when a "Memory Dump" (byte-to-byte copy of the volatile memory) is taken at the crime scene before attempting to shutting down the device's operating system. The process of memory acquisition could mean running a command on the system to capture and store memory to a connected storage device, and while this conflicts with *Principle 1* of the ACPO guidelines as discussed earlier in Sect. 7.2.1, this requirement is addressed by *Principle 2* given that each action is fully and rationally documented with a satisfactory explanation on the CoC.

A digital CoC replaces the paper-based approach, it describes an electronic documentation of this process. Digital CoC can be convenient but more vulnerable to integrity attacks (data alteration), which puts the whole investigation at risk. The solution we discuss in this paper focuses on the utilisation of Blockchain to enable trust, integrity, authenticity, traceability, and verifiability. The attributes and components of a Digital CoC are described and discussed below:

A Distributed Ledger CoC records are distributed to a decentralised computing network system incorporating multiple sources or nodes to store and retrieve these records when needed.

Linked-Blocks To amend the Blockchain with a new CoC record to the ledger, it must include one reference signature (hash) from the previous record in the Blockchain. This way, all records have pointers to other records and are linked in a chronological order. If data in any block is changed (e.g. due to system failure or integrity attack), the hash (as a unique representation of the record) will also change resulting in a mismatch with the recorded reference hash in the consent block. This would break the chain and the overall system would, therefore, reject any altered block.

Network Nodes These are the participating computers. They form and support the distributed environment and perform the mining process to add or verify transactions.

Transactions A transaction in this use case is the process of adding a new CoC record. Adding a new transaction to a distributed interlinked ledger means that copies of the new record will be synchronised with the whole network. This global update indicates the system has no single-point-of-failure, which is an effective countermeasure against availability attacks.

The above can be used to define the Blockchain-based Digital CoC as a distributed ledger formed of blocks of electronically hashed evidence records that are linked together to establish a chain. Evidence records in this context relate to the process of handling acquired crime scene evidence from the time it is seized or collected until the time it is presented to a Court of Law. Nonetheless, the architecture of a Blockchain-based CoC whether for a standard implementation or to enable a CoC for DWs (more discussion in Sect. 7.5) will consist of the following main components:

Evidence Storage This is where the evidence is stored. Requirements could vary because physical evidence entails a special storage facility to avoid data alteration, while the options for electronic data could include the Cloud as a solution.

Digital CoC Enabled through the Blockchain as discussed earlier.

The Interface This component is responsible for enabling communications between all the users. It incorporates access control and evidence management; creating a new record, evidence state verification, and disposal of evidence.

7.5 Blockchain for Forensic-Enabled Electronic Systems: A Case Study in eHealth

Digital systems such as electronic documentation and reporting tools offer the healthcare sector both quality and the required utility to facilitate communication between permissioned stakeholders. Examples of regular stakeholders include healthcare providers, auditors, patients but also incident responders when an investigation is triggered. However, utilising technology without following appropriate guidelines raises serious concerns related to data integrity and compliance with local laws and regulations (Staats et al. 2017). Without measures to enforce documentation integrity and completeness, records cannot be trusted to provide a realistic reflection of the patient condition. There are also several legal issues since this type of data affects the patients' safety and quality of healthcare which leaves the organisation accountable for medical errors (Moffatt-Bruce et al. 2016).

Nonetheless, there are other reasons to extend the requirement beyond maintaining data integrity for the records separately. A CoC is a more appropriate means to create a verifiable series of events in the form of a story to support DFIR. A practical example showing the benefit of establishing a CoC can be demonstrated with Disease Management Programmes (DMP). Over the last two decades, several DMPs have been implemented worldwide in response to the escalating burden of chronic conditions. The implementation of DMPs was an attempt to improve the quality of care for selected chronic conditions that are influenced by lifestyle and behaviour change (Alhaboby et al. 2018). These programs came in different designs and evaluation techniques to deliver a variety of interventions tailored to pre-defined case studies. DMPs can be delivered through a web-based disease management solution. However, studies show evidence that people with long-term conditions and disabilities are frequently labelled as vulnerable, and commonly victimised online. While those victimised patients require instrumental support via DMPs to understand their conditions and empower them to manage their own treatment in everyday life, additional short and long-term consequences related to cyber-victimisation could intensify existing psychological and health complications. For instance, 'distress' as a commonly reported impact of cyber-victimisation could theoretically lead to neurohormonal changes in the blood, increasing cortisol, catecholamine and insulin secretion resulting in increased blood glucose, heartbeat, blood pressure, urination and other changes (Alhaboby et al. 2016). Preserving an admissible evidence for the above requires a connected Forensic-enabled system to be in place. This would then help patients to request help, provide sufficient information to what they go through, and support a legal action to mitigate against cyber-victimisation. A summary of threats and opportunities for this case study would therefore be:

1. Non-adherence to self-management planning is a major instability factor, while DMPs and Online Coaching Programmes are cornerstones to support the stability of long-term self-management for people with long-term conditions.
2. Likewise, we argue the inverse correlation on stability between the impact of cyber-victimisation versus the ability to forensically document all submitted data for such incidents.

The benefit of developing forensic-enabled DMPs introduces many opportunities; Firstly, it gives the victims, or a third-party acting on their behalf, the advantage of supporting a legal action against an attacker to address the source of the problem (Alhaboby et al. 2018). A recent study (al-Khateeb et al. 2017) provides evidence that that victims of cyberstalking accept the idea of third-party intervention as a response to threats. The study also shows that victims seek help from the independent anti-cyberstalking organisations and the Police. In law, preserved incriminating material (e.g. breaking the Protection from Harassment Act 1997 in the UK) supported by a documented incident log in the form of a CoC can be admissible to a Court of Law. Secondly, this information could be sufficient to reduce the time required to recover the identity of the attacker. Thirdly, the evidence could be utilised to support the victim's eligibility for extended instrumental support from national health services. Finally, this level of automation in the documentation process offers an opportunity to implement more accurate methods to assess the risk associated with victimisation attacks.

7.6 Blockchain to Enable Digital Witnesses

7.6.1 Exploiting the Widespread of IoT Devices

The Internet of Things (IoT) is the interconnected network of standard devices such as laptops and smartphones, and non-standard devices such as moving vehicles, software applications, connected fridges (all home appliances), and virtually any connected object. A significant part of this phenomenon is focusing on consumer applications. Smart Homes, as an example, raises many legitimate concerns related to data privacy (Risteska Stojkoska and Trivodaliev 2017) but as the technology emerges further it covers more aspects of our daily living. Our cyber-physical interactions can also be captures by IoT sensors within a connected car, a plane, or via a mobile phone, or digital watch. There are IoT applications to support agriculture, transportation, healthcare, environment and energy management. Holistic frameworks are being proposed (Risteska Stojkoska and Trivodaliev 2017) to incorporate the components of various IoT architectures within a single management model. This type of research towards extending the interoperability (Wan et al. 2014) between IoT devices could be utilised to facilitate further collaboration, in our case, to collaborate on providing event-related evidence within their sensing capabilities.

7.6.2 The Role of a Witness

Rather than discussing the challenges introduced by IoT, in this section, we look at an opportunity provided by this complicated network of devices to facilitate potential witnesses for DFIR. In law, the role of a witness is fundamental, and testimony is a form of evidence obtained from a witness who makes a statement to declare a fact (Smith and Bace 2002). A witness claims to have direct knowledge or information related to the case being considered in court. Witness testimony can be oral or written and is accepted after an oath. Additionally, having an incident witnessed by more than one person increases the validity and assertion that it was a true event. Furthermore, when the witness uses one of their senses (e.g. seeing, hearing, smelling) then they are called "eyewitness", this is in contrary to hearsay, which is to testify that the information was perceived indirectly. For example, it could have been written or said by someone else. Technology could also be utilised, and it is important to note that the use of science and technology by means of an instrument (e.g. microphone) to aid the perception of a human sense is acceptable and is not considered hearsay. At times, the information could initially be captured by an instrument (e.g. recorded in a log by a computer system), in this case, an independent Expert Witness must analyse this electronic data to present the evidence to a Court of Law. In the case of IoT, we argue that IoT devices can act as DWs to provide affirmation towards events related to a crime scene within their sensing capabilities (Nieto et al. 2016). However, a CoC must be maintained for any data generated by these IoT devices to be admissible, and further work in this area is required to standardise the requirements to be met before an IoT device can qualify for the role of a DW.

7.6.3 IoT Devices as Digital Witnesses

The data lifecycle is the sequence of phases data go through from the initial creation until it is finally deleted (Abuosba 2015). Data can be generated from a manual human entry, collected from an external source or captured from the environment (signal reception or sensor data). Through this journey, data could be edited to recreate new data units, or viewed and archived. Data transfer occurs when data units are copied across communication channels. Data, including data remnants, can be used as Digital Evidence and is therefore very important to the digital investigation process if put within the right context for analysis. In the case of forensic acquisition at a crime scene, data, and the medium storing the data are covered by the "identification" and "preservation" stages of the eDiscovery process as demonstrated in Fig. 7.1. The earlier discussion also covered how Blockchain can be utilised to preserve data at these two stages. Therefore, for an IoT device to comply with this process it should first be able to identify records of interest, to log this data (for short or long term), and to transfer the logs to the network system as demonstrated in Fig. 7.2.

Some IoT devices are supported by a data storage facility. For example, CCTV (Closed-circuit Television) are usually configured to stream their recordings or store them locally. However, IoT sensors and actuators require support from additional resources to process and store data. Other applications such as Connected Cars (CC) could include cameras, low-powered sensors and internal storage, but a CC system would still transfer data to the network as an attempt to avoid Denial-of-Service (DoS) attacks or because the internal storage cannot cope with the rate at which new data is generated in the long run. In Fig. 7.3, we show that a DW should have the ability to process and log newly captured data to a Blockchain, but it does not have to store data for a long time, instead, a DW could pass it through to a cloud-based network. A forensic investigator could then acquire a copy from what we call a "Hearsay DW" device. Integrity and authenticity checks can be performed using the hashes and metadata submitted to the Blockchain as part of a digital CoC.

Additionally, IoT devices which are not resource-constraint could provide many other artefacts to contribute to the value or the admissibility of the Digital Evidence as explained below.

Device-Related Identifiers Capturing values such as Device ID, Build No and Kernel version helps to identify the device from which the evidence was captured.

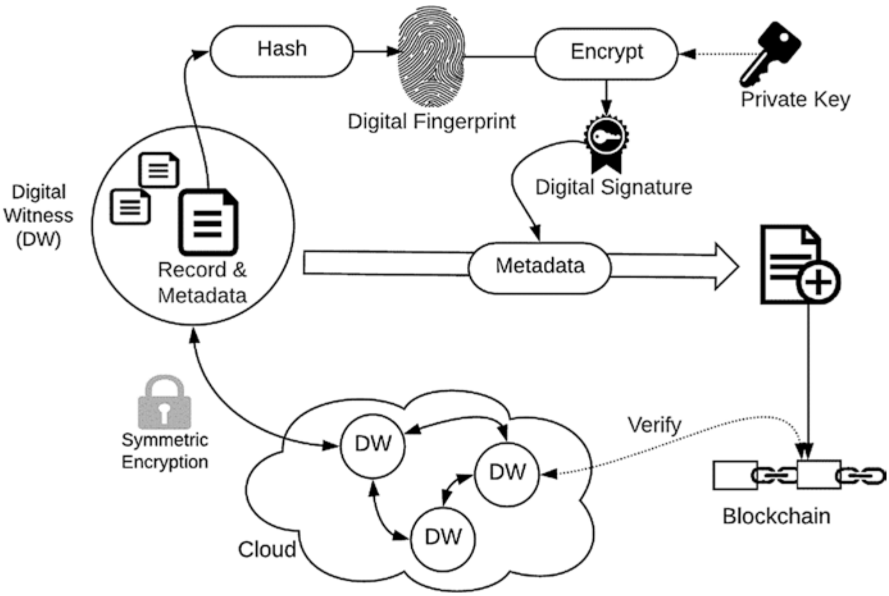

Fig. 7.3 In a DW scenario, data can be identified, signed and sent to one or several Hearsay DW for backup. The cloud can be utilised to facilitate data availability. Metadata is signed by the IoT device private Key to maintaining authenticity

Location Indicators GPS coordinates, connected Wi-Fi and Network Operator data can be invaluable to recover the location of an incident captured by a nearby DW.

Time-Related File system timestamps show the time when each file was created, accessed and modified.

Security Indicators Devices should be designed to self-report any integrity check concerns related to their internal workings of the DW itself. This can be the outcome of misconfiguration or a Malware infection (Irshad et al. 2018).

Integrity Checks Captured data must be hashed to maintain the integrity of the file at the time of acquisition or submission. Multiple hashes are recommended to avoid errors within this process. Examples of hash functions currently used include MD5, SHA-1, SHA-512 and SHA-256.

The Digital Evidence in traditional cases is documented by a qualified Digital Investigator. This is a typical admissibility requirement included within guidelines such as the principles published by the Association of Chief Police Officers (ACPO) in the UK. Therefore, for forensic readiness to be maintained, the software should automate the process of data acquisition with reference to these principles, and the software code should go through a review process to meet the reliability requirement with reference to standards (e.g. the Daubert standard).

7.7 Conclusions

Blockchain has shown its potential to support computer systems with a tamper-proof series of timestamps making it a suitable facilitator to establish a strong digitalised Chain-of-Custody (CoC). The distributed nature of the technology makes it resistant to various cyber-attacks against the availability and integrity of its data. These advantages are most suitable for DFIR to develop new approaches in the fight against cybercrime. We have explored and discussed various implementations making Blockchain very useful to digital investigators. Additionally, we have reviewed how the digital investigation and eDiscovery models have emerged over time, this was important to demonstrate how Blockchain could effectively support an innovative deployment for the "identification" and "preservation" phases of this process. Thereafter, the concept of Digital Witnesses (DWs) was introduced to show how we can exploit IoT devices to automate the identification and preservation of Digital Evidence. The aim was to cover incidents as they happen from several angels (this would depend on the number and nature of available DWs). To qualify as DW, IoT devices should have solid security features such as an embedded Trusted Computing Hardware to periodically verify its integrity.

In conclusion, IoT extends the Internet beyond standard devices to include appliances we have at home, vehicles we use to travel, and wearable devices such as watches and digital trackers. This introduces various challenges on top of which is privacy implications. However, privacy and DFIR are two confronting disciplines. Therefore, in this work, we look at the opportunities provided by the increasing number of IoT devices. Particularly, we looked at a new approach where a Blockchain-based Chain-of-Custody can be established at the same time pre-identified data (data of interest) is generated by an IoT device. The data of interest can be about the device itself, other IoT devices or the environment around. This will provide a new level of forensic readiness. That said, more work is needed in this area to cover topics including but not limited to data governance, standardisation of DW admissibility, and the trade-off between DW and user privacy.

References

Abuosba K (2015) Formalizing big data processing lifecycles: acquisition, serialization, aggregation, analysis, mining, knowledge representation, and information dissemination. 2015 international conference and workshop on computing and communication (IEMCON), pp 1–4. https://doi.org/10.1109/IEMCON.2015.7344533

Alhaboby ZA, Al-Khateeb HM, Barnes J, Short E (2016) The language is disgusting and they refer to my disability: the cyberharassment of disabled people. Disabil Soc 31(8):1138–1143. https://doi.org/10.1080/09687599.2016.1235313

Alhaboby ZA, Alhaboby D, Al-Khateeb HM, Epiphaniou G, Ismail DKB, Jahankhani H, Pillai P (2018) Understanding the cyber-victimisation of people with long term conditions and the need for collaborative forensics-enabled disease management programmes. In: Jahankhani H (ed)

Cyber criminology. Advanced sciences and technologies for security applications. Springer, Cham

al-Khateeb HM, Epiphaniou G, Alhaboby ZA, Barnes J, Short E (2017) Cyberstalking: investigating formal intervention and the role of corporate social responsibility. Telematics Inform 34(4):339–349. https://doi.org/10.1016/j.tele.2016.08.016

Cocco L, Pinna A, Marchesi M (2017) Banking on Blockchain: costs savings thanks to the Blockchain technology. Futur Internet 9(3):25

Daryabar F, Dehghantanha A, Choo K-KR (2017) Cloud storage forensics: MEGA as a case study. Aust J Forensic Sci 49(3):344–357. https://doi.org/10.1080/00450618.2016.1153714

Irshad M, Al-Khateeb HM, Mansour A, Ashawa M, Hamisu M (2018) Effective methods to detect metamorphic malware: a systematic review. Int J Electron Secur Digit Forensics 10(2):138–154. https://doi.org/10.1504/ijesdf.2018.090948

Johng H, Kim D, Hill T, Chung L (2018) Using Blockchain to enhance the trustworthiness of business processes: a goal-oriented approach. 2018 IEEE international conference on services computing (SCC), pp 249–252. https://doi.org/10.1109/SCC.2018.00041

Ma A (2018) Thousands of people in Sweden are embedding microchips under their skin to replace ID cards. http://uk.businessinsider.com/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5?r=US&IR=T

Mengelkamp E, Notheisen B, Beer C, Dauer D, Weinhardt C (2018) A Blockchain-based smart grid: towards sustainable local energy markets. Comput Sci Res Dev 33(1):207–214. https://doi.org/10.1007/s00450-017-0360-9

Moffatt-Bruce SD, Ferdinand FD, Fann JI (2016) Patient safety: disclosure of medical errors and risk mitigation. Ann Thorac Surg 102(2):358–362. https://doi.org/10.1016/j.athoracsur.2016.06.033

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

Navarro-Ortiz J, Sendra S, Ameigeiras P, Lopez-Soler JM (2018) Integration of LoRaWAN and 4G/5G for the industrial internet of things. IEEE Commun Mag 56(2):60–67. https://doi.org/10.1109/MCOM.2018.1700625

Nieto A, Roman R, Lopez J (2016) Digital witness: safeguarding digital evidence by using secure architectures in personal devices. IEEE Netw 30(6):34–41. https://doi.org/10.1109/MNET.2016.1600087NM

Pollitt M (2010) A history of digital forensics. In: Advances in digital forensics VI. Springer, Berlin/Heidelberg, pp 3–15. https://doi.org/10.1007/978-3-642-15506-2_1

Risteska Stojkoska BL, Trivodaliev KV (2017) A review of internet of things for smart home: challenges and solutions. J Clean Prod 140:1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006

Smith FC, Bace RG (2002) A guide to forensic testimony: the art and practice of presenting testimony as an expert technical witness. Pearson Education

Staats BR, Dai H, Hofmann D, Milkman KL (2017) Motivating process compliance through individual electronic monitoring: an empirical examination of hand hygiene in healthcare. Manag Sci 63(5):1563–1585. https://doi.org/10.1287/mnsc.2015.2400

U.S. Department of Homeland Security – United States Secret Service (2015) Best practices for seizing electronic evidence: a pocket guide for first responders

Wan J, Zou C, Zhou K, Lu R, Li D (2014) IoT sensing framework with inter-cloud computing capability in vehicular networking. Electron Commer Res 14(3):389–416. https://doi.org/10.1007/s10660-014-9147-2

Williams J (2012) ACPO good practice guide for digital evidence. Metropolitan Police Service, Association of chief police officers, GB