Adopting blockchain technology to protect the integrity of electronically stored evidence

Aleksander Gjerrud

M00647726

Supervisor: Sukhvinder Hara

04.10.2018

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Science in Electronic Security and Digital Forensics.

ABSTRACT

Maintaining the integrity of digital evidence can be a tedious and time-consuming effort which require strict documentation and attention to detail. This project covers one of the most crucial parts of the digital investigation process, namely preserving the integrity of the digital evidence. Insufficient methods and procedures in handling evidence might render it inadmissible in court, effectively making it unusable, even if it contains decisive material to the case. This report deals with several important aspects of the preservation stage of the evidence handling process. It covers the phases from imaging and hash computation of the first acquisition, to protective storage of the hash value and digital signatures, to maintaining the chain of custody and admissibility in court. Going further on the technical implementation, the report discusses blockchain technology and consensus mechanisms, and the storage of the physical aspect of digital evidence and electronic tag implementation. Integrating blockchain technology into the chain of custody allows it to gain functional attributes beyond that of a regular audit trial. The capabilities of the blockchain is transferred to the chain of custody, giving it immutability, distributed redundancy among nodes, and transparency for all the nodes in the network. The added functionalities provide more trust among users as well as increased security on the network that is documenting the evidence process.

ACKNOWLEDGEMENTS

I would like to express my gratitude towards all the people who supported me throughout this project. I would like to offer my special thanks to my supervisor Sukhvinder Hara for her support and guidance in completing this complicated task, and for her effort as an educator. My appreciation is further extended to Dr. Panos Giannopoulos and Prof Raja Nagarajan as well as the course module leader Dr. Carlisle George for generous assistance and advice through the course and the degree. I would also like to thank my peers with special regards to Noritaka Tauchi for keeping me company and contributing whenever there were questioning to be answered. Finally, I wish to thank the people who participated in the interview process on short notice and provided constructive feedback using their own professional views and opinions.

CONTENTS

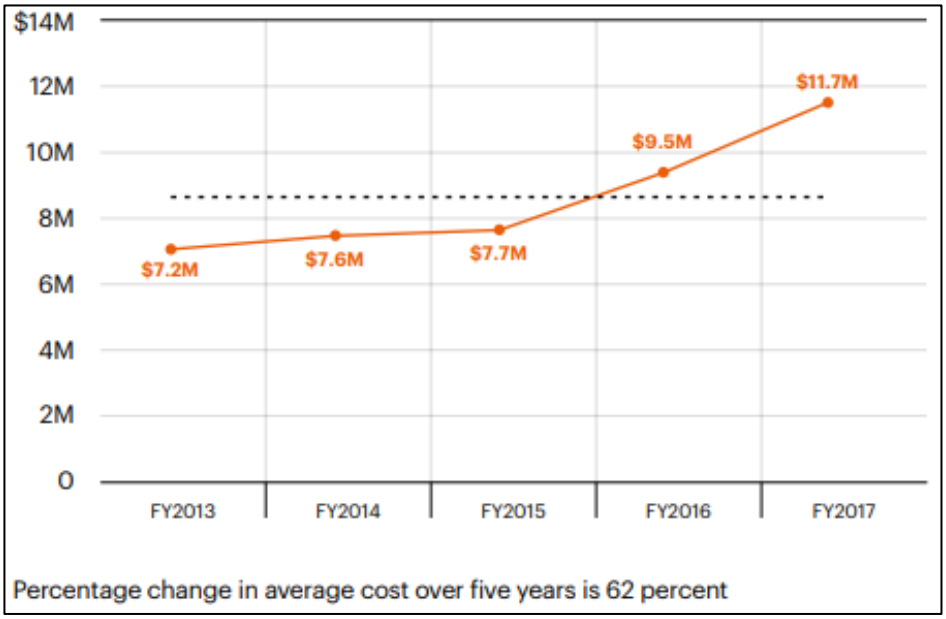
CHAPTER 1: INTRODUCTION

Computers are being used more than ever to commit crimes. An assessment on cybercrime issued by the NCA (National Crime Agency, 2016) reported in their findings from 2015 that the amount of criminal activity involving computers has dethroned conventional crime as the major part of total crime in the UK. The assessment reports that this was the first time the ONS (Office of National Statistics) included cybercrime in the annual Crime Survey for England and Wales. Cybercrime in the report consists of both cyber dependant crime (can only be committed using computers) and cyber-enabled crime (can be conducted offline as well as online, but is happening online at a larger scale). The ONS estimated 2.46 million cyber incidents in UK in 2015 with only approximately 16,000 cyber-dependant and 700,000 cyber-enabled incidents reported to Action Fraud over the same period. According to the ONS 2015 numbers, cyber-crime takes over as the larger proportion of total crime in the UK.

Removal of traditional physical boundaries and international borders has let the internet increase the potential for traditional crime and technology-specific activities (Britz, 2013, p. 17). A report published by Accenture (2017) writes about the cost of cybercrime. From one of their findings it is shown that the global average cost of cybercrime is increasing (figure 1). According to these findings, there has been an 62% increase in the cost of cybercrime from 2013 to 2017 on a global average in 254 separate companies across countries, organisation size, and industry.

This increase in cybercrime makes it necessary for law enforcement and digital investigators to build competence to handle such crimes. Computers are ubiquitous within modern organisations and with its widespread use, it is inevitable that illegal activities will involve computers (Kruse II & Heiser, 2001, p. 2). With rise in computer usage and how more people are learning how to properly take advantage of the technology, we must be prepared for the criminal activities that follows. Now that computer technology is commonplace, as are crimes in which computers are the instrument, target, and by nature also the location where the evidence is stored (Nelson, Phillips, & Steuart, 2015, p. 6).

Figure 1



Although computer forensics has aspects similar to other forms of forensics, it require knowledge of computer hardware, software, and proper techniques to avoid compromising or destroy evidence (Solomon, Rudolph, Tittel, Broom, & Barrett, 2011, p. 2). The operations used to collect, analyse, control, and present electronic evidence cannot modify the original item in any manner. The nature of computer and electronic evidence poses special challenges for its admissibility in court proceedings and corporate security investigations (Newman, 2007, p. 4). Any alteration to the primary source of evidence could contaminate it and make it inadmissible in court (Volonino, Anzaldua, Godwin, & Kessler, 2006, p. 67). Evidence handling is a crucial topic for people involved in the investigation and the overall case surrounding it. The entire investigation is of little value if the evidence pointing to a guilty defendant is not allowed into the trial or is given little evidential weight. Proper handling is an important issue facing all criminal investigators, and because of its nature, cybercrime investigations in particular (Shinder & Tittel, 2002, p. 546).

To secure evidential integrity, investigators are encouraged to utilise an audit trial to prove that the evidence was never changed and always accounted for. The chain of custody is a guideline for handling evidence, and ensures that the evidence being presented are the same evidence that was originally seized by recording how it was handled, who handled it, and documenting the integrity of the evidence that was collected (Volonino et al., 2006, p. 68).

The integrity of digital evidence is usually secured with safe physical storage and by making a hash value of the data it stores. Adam Stone (2015) describes hash as an algorithm to create a unique digital impression of a digital record; any change to that record afterwards will result in a new unique hash. This protects the integrity of the stored data because any modifications to the evidence also will modify the hash, causing a mismatch of the original hash value. This is only a secure method if the hash is securely stored as well. Access to the stored hash leaves it vulnerable to tampering.

A way of securing the information regarding the evidence is to store it in a system integrating blockchain technology. As described by Ed Fowler (2018), the three main functions of blockchain are decentralisation, immutability, and control. Decentralisation is a security measure spreading a redundancy of copies which are connected in a network to make sure there are no single point of failure. Immutability is achieved as the consisting blocks are linked together and therefore cannot be altered without breaking the integrity. Control mechanisms can be implemented to restrict or grant access to the contents. How these key areas operate are further discussed throughout the project.

Information about evidence can be stored within the blockchain to prevent tampering. This especially counts for digital evidence as the hash value will be stored, making sure the evidential integrity stays intact. All actions done in the blockchain can be historically accessed and viewed making the system transparent for the involved parties and users.

Several entities have begun to investigate and develop into the idea of using blockchain to store information. Some organisations are additionally looking to develop systems for evidence and data integrity. Kinesense and Evident-Proof are two organisations working with systems integrating hashing and blockchains for data integrity preservation. Simple searches for blockchain online also reveals a multitude of results showing a clear interest in the adaptation of blockchain for integrity driven systems.

This project is meant to get an understanding of how blockchain may assist in storing electronic evidence and evaluate the possibility of using this blockchain technology to secure the integrity of digital evidence. It may not serve as a complete or permanent solution to complement evidence security systems, but is worth to analyse and consider as an implementation to improve existing or newly developed systems. Existing approaches to securing evidence integrity will be discussed throughout the report as well as identification of existing usages of blockchain technology. This will lead to an assessment and analysis of the usability of the blockchain as a protective means to store information and preserve data integrity.

CHAPTER 2: BACKGROUND

This project may involve topics and areas which are new to some readers. This chapter is meant to describe the major topics this paper is based upon in context and purpose of the report.

2.1 Digital evidence

To properly investigate an incident and build a case that allows actions to be taken against a perpetrator, we need evidence as proof of the perpetrator's identity and actions. Computer evidence consists of files and contents that remain after an incident has occurred. There are four basic types of evidence that can be used in a court of law. These types are real evidence, documentary evidence, testimonial evidence, and demonstrative evidence. Computer evidence generally falls into the first two categories. (Solomon et al., 2011, pp. 56–57). As with categories of evidence, there are also four basic situations where a computer is involved in some type of crime (Newman, 2007, pp. 4–5). The computer is the target of come illegal activity, it is the medium through which the illegal activity is committed, it is incidental to the commission of the illegal activity, or a combination of the previous three situations. When a computer, a network, or other electronics are involved in a case that is being investigated, it may be regarded as electronic evidence. The International Organisation for Standardisation (2012) ISO/IEC 27037:2012 standard defines the term of digital evidence as information or data, stored or transmitted in binary form that may be relied on as evidence. This project is focused on the evidential material that is in digital form.

2.2 Digital forensics

Digital/ computer forensics is the fundamental topic of this project. It is the processes and sciences which utilise digital evidence to find answers and reach conclusions regarding different cases the evidence is connected to. There is no single definition of neither digital nor computer forensics.

> *"Digital forensics, also known as computer and network forensics, has many definitions. Generally, it is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."* (National Institute of Standards and Technology: Kent, Chevalier, Grance, & Dang, 2006, p. ES-1)

The U.S Department of Defence (DoD) released a directive for the DoD Cyber Crime Center (DC3) including their definition of digital forensics as following:

> *"In its strictest connotation, the application of computer science and investigative procedures involving the examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony."*
> (Department of Defence, 2010, p. 13)

Most definitions of digital forensics are created and described as suited best for the particular purpose of the creator. Robert C. Newman (2007, p. 5) writes computer forensic science as the science of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on a computer media. The description and definition may differ to an extent, but they mostly cover all the important areas surrounding digital forensics. Bill Nelson et al. (2015, p. 137) writes that the most general tasks investigators will come across when working with digital evidence include:

- Identification of digital information or artefacts that can be used as evidence
- Collect, preserve, and document evidence
- Analyse, identify, and organise evidence
- Rebuild evidence or repeat a situation to verify that the results can be reproduced reliably

The contents of this project are narrowly focused in on the single key factor that is common in most definitions of digital forensics, namely preserving the integrity of the acquired data. This is one of the most crucial stages in any case to maintain the evidential weight of the data and to ensure that the evidence may be admissible to assist the case. This project is focused on the methods used to provide the necessary security needed to protect the integrity of the collected electronic evidence.

2.3 Admissibility of evidence

Any evidence to be used in a potential court case must be relevant and admissible. Relevant evidence means it must stand to either prove or disprove aspects of the case while admissibility means that the evidence conforms to all regulations and statues governing the nature and the manner in which it was obtained and collected (Solomon et al., 2011, p. 71). As with traditional investigations, collections and preservation of all evidence must be done with caution to assure court admissibility. Evidence seized without a proper warrant issued may instantly render it inadmissible and will leave the investigation with one less item to assist in the prosecution of the suspect (Britz, 2013, p. 322). When handling evidence, always having in mind the assumption that the evidence will be used in court tends to make people more diligent in adhering to evidence handling and the including procedures (Solomon et al., 2011, p. 73). The preservation of any evidence in its original form is one of the most important stages to have control of the incident being investigated. Any modification to timestamps or the data itself must be avoided as the evidence may be deemed inadmissible, and the defence may use this as an argument to have such tainted evidence removed (Newman, 2007, p. 5). Evidence deemed inadmissible may be worse than just being excluded from the case. Not only may obtaining material through illegal search and seizure destroy the prosecution's case, effectively letting a criminal go free, but can also cause actions to be taken against the people who violated set rules when collecting evidence (Shinder & Tittel, 2002, p. 587). Forensics may be slow process, but a trained investigator should be reasonably assured that most of the incriminating evidence will be found and admissible by following a standard set of rules relating to their respected field (Schultz & Shumway, 2001, p. 175).

2.4 Evidence integrity preservation

Unlike conventional physical evidence, storing electronic evidence in a safe, protected, and guarded facility might not be adequate to protect the data it stores. The collection and preservation of digital evidence differ in nature from most other types of evidence and thus require different methods of handling. For this reason, standards within computer forensics have been developed for this specific process, which includes proper and accepted procedures vital to a successful case (Shinder & Tittel, 2002, p. 546). The International Organisation for Standardisation (2012) have set out the ISO/IEC 27037:2012 standard named "Guidelines for identification, collection, acquisition and preservation of digital evidence". A couple years after, the Scientific Working Group on Digital Evidence (SWGDE, 2014) published a best practices document to describe the practice for collecting, acquiring, analysing, and documenting data that has been found during a computer forensics examination. Both organisations do additionally have several other documents relating to the forensic processes ranging from acquisition, to image authentication, to transportation and storage of items. The Association of Chief Police Officers (ACPO) have agreed upon the "ACPO Good Practice Guide for Digital Evidence" (Williams, 2012) to be adopted by police forces in England, Wales, and Northern Ireland as the primary guideline for UK law enforcement personnel who may deal with digital evidence.

In any investigatory work, records should be kept of all activities and findings as work progresses. For this purpose, a journal should be maintained to record steps taken as evidence is processed. The goal is to enable reproduction of the same results when the investigator or other parties repeat the steps originally taken to collect the evidence (Nelson et al., 2015, p. 160). Uncertainties and questions would arise if evidence could not be found using the same techniques as the original collector of the evidence. The National Institute of Standards and Technology (NIST) require for both repeatability and producibility. Repeatability require that the same results should be obtained using the same methods, on identical items, in the same

laboratory, by the same operator, using the same equipment. The reproducibility condition required that the results are obtained with the same methods, on identical items, in different laboratories, with different operators using different equipment (Newman, 2007, p. 9).

All evidence presented in a court of law must exist in the same condition as it did when it was collected. Evidence must be in pristine condition as it cannot be allowed to change at all once it has been collected. Evidence must be provided to prove the fact that the evidence exists, without changes, as it did when it was collected. This documentation surrounding every move and access of evidence and is called the chain of custody (Solomon et al., 2011, p. 65). Chain of custody is a term referred to as the continuity of evidence. The evidence must be able to be traced throughout the investigation from initial collection until presentation in court. Any break to the chain of custody allows for allegation such as evidence tampering or that other evidence has been substituted for it (Shinder & Tittel, 2002, p. 583). A properly documented procedure is important, and evidence could be thrown out of the court if it cannot be duplicated consistently. The chain of custody begins when the first responder enters the scene and must ensure the protection and documentation of the evidence (Newman, 2007, p. 6). This procedure documents the complete journey of the evidence during the life of the case and should include answers to questions such as; who the collector is, how and where, who took possession of it, how it was stored and protection in storage, and who took it out of storage and why (Kruse II & Heiser, 2001, pp. 6–8). This type of audit trial is effective in providing both admissibility and integrity to the evidence.

Digital evidence can be classified as original digital evidence and duplicate digital evidence. The original refers to the physical items and data objects associated with those items at the time it was seized and the duplicate refers to an accurate digital reproduction of all the data objects contained on the original item (Shinder & Tittel, 2002, p. 550). Integrity must be maintained of the digital evidence in the lab as it when collected in the field. The first task is to preserve the data and create a forensically sound copy of the evidence as quickly as possible (Nelson et al., 2015, p. 160). The “mirror image” of the data should be an exact duplicate of the original, and the original evidence items should be stored in a safe place where its integrity can be maintained (Shinder & Tittel, 2002, p. 558). This image copy is also known as a bit-stream copy, bit-for-bit copy, or forensic copy. It creates an exact duplicate of the original drive, medium, or data that is used (Nelson et al., 2015, p. 37). Investigators should always work from an image in order to preserve the original evidence. This counters defence challenges and negates the possibility of both accidental and intentional data destruction and manipulation (Britz, 2013, pp. 285–286).

Proving that no data changed after collection can be challenging even with a chain of custody present. Digital evidence has an advantage in this context by being able to show that the evidence did not change after collection (Kruse II & Heiser, 2001, p. 13). Computer crime investigators gather digital evidence that needs to be preserved and verified in the future. An examiner will run a “hash” utility against the evidence and save these values to be able to demonstrate that no data was manipulated from the time of collection to the time the evidence is presented (Kruse II & Heiser, 2001, p. 90). Hashing is a cryptographic technique that provides both integrity and timestamping to data. A common description of hash is that it is calculating a value that function as an electronic fingerprint for either individual files or entire disk drives (Kruse II & Heiser, 2001, p. 13), while a technical description of hashing would be that the function works by mapping binary strings of arbitrary length to binary strings of some fixed length (Menezes, Oorschot, & Vanstone, 1996, p. 33). Message Digest-5 (MD5) and Secure Hash Algorithm (SHA) family are the most used forms of hashing as of today. SHA were originally developed by the National Security Agency (NSA) as a published U.S. government standard and can through different versions produce higher bit message digests (hash) than MD5 is capable of (Newman, 2007, p. 124). In the context of digital forensics, the functions of these types of hash algorithms is to assist in the repeatability requirement of evidence discovery and the integrity of the data involved.

2.5 Blockchain

The first version of what came to be known as blockchain technology was introduced in a paper by Stuart Haber and W. Scott Stornetta (1991) when they published a paper on "How to Time-Stamp a Digital Document". This document included techniques which is recognisable in the modern blockchains, such as time-stamping, hashing, digital signatures, linking tasks sequentially, and distributed trust. Satoshi Nakamoto (2008) later published a paper named "Bitcoin: A Peer-to-Peer Electronic Cash System" and would successfully later on implement the methods used to make such a system, without the necessity of a third party to intervene in the processes. The blockchain in the Bitcoin perspective was originally created as "…an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 2008, p. 1).

The name Satoshi Nakamoto is believed to be a pseudonym as no one knows the identity of the Bitcoin creator to this date. Nakamoto remained active in the Bitcoin community until 2011 before handing over the development of Bitcoin to its core developers and disappearing without any form of communication. The term "chain of blocks" in Nakamoto's paper later evolved over the years to simply become "blockchain" (Bashir, 2018, p. 16). Imran Bashir (2018, p. 16) provides a layman and a technical definition of the term. For the common definition he describes it as *"…an ever-growing, secure, shared record keeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update"*. He further technically and more accurately defines the blockchain term as "*…a peer-to-peer, distributed ledger that is cryptographically-secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers"*. The technical definition includes several key words important to the topic. This chapter will avoid in-depth explanation of these attributes but rather utilise the descriptions used by Bashir (2018, pp. 16–17) to a lesser extent:

Peer-to-peer: Network has no central control, meaning all users talk to each other directly.

Distributed ledger: The ledger is spread/shared among all peers in the network. Each peer holds a complete copy of the ledger.

Cryptographically-secure: Cryptography is utilised to secure services which makes the ledger secure against tampering and misuse. Cryptography is the study of mathematical techniques and relates to information security in the sense of confidentiality, data integrity, and data origin and entity authentication (Menezes et al., 1996, p. 4).

Append-only: Refers to the fact that data can only be sequentially added to the blockchain. Once data has been added it is almost impossible to change it, making the chain practically immutable.

Consensus: Updates are done only after consensus among the peers/ nodes in the network has been made. This is done through validation of strict criteria defined by the blockchain protocol. This functions as an agreement of the final state of the data on the blockchain network between all parties. There are different kinds of consensus for a variety of control.

The basic composition of the blockchain lies in the addresses, the blocks, and the transactions it consists of. Those are a part of the generic elements to come across when discussing blockchains. Addresses are used as unique identifiers in blockchain transactions to represent senders and recipients. They are usually represented as a private key or derived from one (Bashir, 2018, p. 21). Public key cryptography uses two distinct keys called the private key and the public key. From this key pair, the public key may be shared with others, while the private key need to be kept hidden from anyone but the user. The key pair are mathematically related and enables encryption with one key and decryption with the other (Windley, 2005, p. 36). Transactions are the fundamental units of the blockchain. They represent a transfer of value from one address to another. The blocks are composed of multiple transactions and elements such as the hash of the previous block, timestamp and other information (Bashir, 2018, p. 21). Timestamping is a basic function which permanently registers the time an action took place on

the blockchain (Mougayar, 2016, p. 40). The reason the data is basically unalterable is because of the hash functions implemented into the blockchain. Reversing hash into a data source is effectively impossible for input data of any complexity. The blockchain's interlinked set of hashes therefore makes it extremely difficult because each block references to the previous record's hash (Liu, 2017).s

CHAPTER 3: LITERATURE REVIEW

The topic of combining blockchain and forensics is still fresh to this date. Several sites and organisations are still considering the idea, and discussions within the area is still going on after being a hot topic for the recent years. There are few organisations publicly showing or writing about working blockchains for this purpose, however, recently people have discovered useful implementations of blockchain technology in other settings where digital preservation, distribution, and trust are key factors. This chapter is focusing in on the published writing and organisations who are discussing the area and the ones who have a service utilising blockchain for data integrity preservation purposes. Assessments regarding a potential functional program or service offered by an organisation may be overly broad and complex, extending to areas not meant to be covered in this report. Services offering such technology will be discussed and reviewed to the extent pursued in this project, specifically how the service solves for the preservation of electronic evidence integrity.

3.1 Existing approaches to integrity protection

A few existing approaches to integrity preservation were introduced in the previous chapter as part of handling evidence after collection. The three most common approaches include; the making of bit-by-bit images of the evidence, an early calculation of the evidence hash value, and to maintain a strict chain of custody. In this part we investigate how people and organisations go about their best practices and professional opinions on how to maintain the evidential integrity.

Chet Hosmer (2002) writes about different ways utilised to prove the integrity of digital evidence. He illustrates the methods, their advantages, and disadvantages using a table format.

Table 1

Method	Description	Types	Advantages	Disadvantages
Checksum	Checks for errors in digital data. Typically, a 16- or 32-bit polynomial is applied to each byte of data, resulting in a 16- or 32-bit integer. The same polynomial can be applied to the data in the future and be compared with the original.	CRC 16 CRC 32	• Easily computable • Fast • Small data storage • Useful for detecting random errors	• Low assurance against malicious attacks • Simple to create new data with matching sum • Checksum must be in secure storage • No identity bound to the data • No time bound to the data
One-way hash	Protects digital data against unauthorised change. The method produces a fixed length integer value representation of the data. It said to be one-way because of the difficulty of constructing new data resulting in the same hash.	SHA-1 MD5 MD4 MD2	• Easily computable • Can detect random errors and malicious alterations	• Hash must be contained in secure storage • No identity bound to the data • No time bound to the data
Digital signature	A method of binding the signer's identity with the data. This method uses a public key crypto-system where the secret key is	RSA DSA PGP	• Binds identity to the data • No unauthorised regenerations	• Slow • Protection of private key • No time bound to the data

	used to generate the signature.		of signature unless private key is compromised	• Can cause invalid signature if the key is compromised or certificate expires

After putting the common methods forward, Hosmer continues to add time as an element to prove evidence integrity. He intends to use this method to answer the questions of when the digital evidence was signed and for how long we can prove the integrity of the evidence that was signed.
Homes concludes with the hope for a new level of digital evidence protection by allowing us to bind the "who" with the "when" and the "what", referring to the digital signer, the time of the signing, and the data we are trying to protect.

A special NIST publication (Kent et al., 2006, sec. 4.2.2) presenting recommendations towards forensic techniques writes about how to ensure data file integrity when managing digital files. For assurance of unaltered files via system connections, they recommend the utilisation of hardware- or software write-blockers to avoid the chance of modification when evidence is connected to a computer for further processing. Solomon et al. (2011, pp. 74–75) explains that when using a write-blocker, normal read access to the device is supported, but all write requests are blocked. Solomon additionally specifies that the difference in a hardware- and a software write-blockers lies in the physical connection of hardware and the opposingly added software layer between the operating system and the disk device driver. The NIST recommendations continues to point out that write-blockers are used when performing backup or imaging to avoid alteration to the data. Their next step involves hash computations and comparisons between copy and original. It states that a hash computation should be done three times during the process. First time before the imaging is performed, second when the image copy is to be compared against the original to ensure a perfect copy, and thirdly to double-check the original to make sure that the process of imaging did not alter it in any way.

Going further on the subject, Jasmin Ćosić and Miroslav Bača (2010b, pp. 429–432) reviews methods to prove digital evidence integrity. Their paper suggests to secure integrity by finding methods based on the "five W's and one H", referring to the "what", "when", "who", "why", "where", and "how" questions of the investigation. Finding answers to these questions will provide proof of the chain of custody by knowing all the details of how evidence was handled throughout the investigation. The solutions proposed involves a digital evidence management framework (DEMF) consisting of a few factors. The suggested framework is set up similar to a function and covers the "what", "who", "when", and "where" of the evidence as such:

```
DEMF = f {fingerprint _of _file,          //what
          biometric_characteristic,       //who
          time_stamp,                     //when
          GPS_location};                  //where
```

The "what" is solved through utilising a hash algorithm to protect the data integrity of the evidence. This factor is intact as long as the hash value has not changed since the last time it was computed. The "who" is normally implemented using a digital signature through an asymmetric cryptographic key pair, but because of the key management, certificate expiration, and other factors, the authors prefers biometrics to sign the digital evidence. The "when" and "where" is provided via timestamping and GPS location technology respectfully. For the last two factors of "why" and "how" is left for the professional investigators to figure out.

Ćosić and Bača (2010a) builds on the idea of exploring the possibilities surrounding digital evidence integrity. In their paper regarding proving chain of custody and digital evidence

integrity with timestamp, they included a table listing out the common methods used to provide integrity to evidence. Extending the table to Hosmer (2002), they have included several additional types which are more up to date with today's solutions:

Table 2

Method	Length	Description	Advantages	Disadvantages
Cycling redundancy checks (CRC): CRC 16 CRC 32 CRC 64	 16-bit 32-bit 64-bit	Often used to verify data in file transfer	Simple and fast. Gives small data in output.	Not as secure as other methods. Easy to generate resulting in the same CRC.
Cryptographic hash function: MD2 MD4 MD5 SHA1 SHA224/256 SHA384/512	 128-bit 128-bit 128-bit 160-bit 224/256-bit 384/512-bit	Mathematical calculation to generate a value based on the input data. Often referred to as the hash value.	Easily comparable to other hash values.	Collision and preimage attacks. Attacks are less probable using SHA224/256 or SHA384/512.
Digital signature	Depending on the hash function.	Resulting hash is encrypted with a private key to later verify the file integrity using the hash value and the public key.	Binds identity to the integrity.	Slow and complex to implement.
Timestamp	Depending on the hash function.	Used for event logging and system file metadata. Trusted timestamping is the process of keeping creation and modification data secure.	Binds data and time with the integrity.	Complex to implement and dependent on the available timestamp service.
Encryption	Depending on the algorithm.	The process of transforming information using algorithms to turn plaintext into cyphertext. Encryption is used to protect confidentiality.	Highly secure.	Slow and complex to implement and maintain.
Watermarking	Depending on the algorithm.	The process of embedding information into another object or signal.	Security and simplicity.	Users cannot alter files without sacrificing quality and utility of the data.

A reappearing subject in the Ćosić and Bača paper is the human factor. Knowing all the different entities interacting or accessing the evidence during the evidence's life cycle, measures such as the ones descried here are important to assure the integrity of the evidence. The examples of human factors mentioned include but is not limited to; first responders, forensic investigators, court expert witness, law enforcement personnel, police officers, victims, suspect, passer-by, and more. The paper suggests a timestamping authority as a trusted third party to prove existence of evidence at certain times. This would also allow us to have a record of all the

times an evidence was being accessed at any stage of the investigation and remove the possibility of backdating timestamps either accidentally or intentionally.

Moving over to practices, the Scientific Working Group on Imaging Technology (SWGIT, 2010) section 13 documents best practices for maintaining integrity of digital images and digital video. As stated on the SWGIT homepage, its operations were terminated as of May 2015 but their guidelines and documentation are still available and is still relevant (SWGIT, 2015). The Scientific Working Group on Digital Evidence (SWGDE, 2017) later on published an altered version containing best practices for maintaining the integrity of imagery. SWGDE covers the same methods as described in SWGIT in a similar manner and it is the most recently reviewed and updated document of the two. Section seven and eight of the SWGDE publication covers methods for maintaining integrity and methods for evaluating integrity. The methods mentioned in the publication are:

Table 3.

Methods for maintaining integrity	
Written documentation	Collection of standard procedures for documenting steps taken to secure the evidence properly (e.g. chain of custody)
Physical security/environment	Mechanical or physical systems to prevent unauthorised access (e.g. personnel control)
Redundant physical copies	Duplicates of files kept in alternate locations to prevent a single point incident
Logical security (WAN/LAN)	Operating system or software to prevent access to files (e.g. passwords, firewalls)
Third-party storage	Transferring files to third parties. This will relinquish control of the integrity and though it may be appropriate in certain cases, methods for access and integrity demonstration independent of the vendor should be in place. Contracts to clarify the vendor's obligations should be expressed before any file transfer.
Digital signatures	The resulting value of a hash computation is signed and encrypted using a private key. File integrity can be verified using the hash and the validation of the source can be checked using the public key. The source of the file can this way be connected to an entity.
Watermarking	A process modifying the contents of the file can even persist as part of the file. It can visually obscure the file and is therefore not widely recommended.
Encryption	Encoding the content of the files to limit access. It alone does not protect integrity but can help in assisting other methods for integrity verification.
Methods for evaluating integrity	
Hash verification	Mathematical calculation generating a hash value based on input data. It is sensitive to changes in input data and should be performed before and after a copy process is done.
Visual verification	Confirming accuracy through visual inspection of the item. Involves the viewing of both the original and the one in question to verify that they contain the same identical visual information.

Evaluation of factors listed in the methods for maintaining integrity	May or may not provide with additional information for verification capabilities. Depends on the integrity process which are in place and implemented.

3.2 Blockchain for integrity purposes

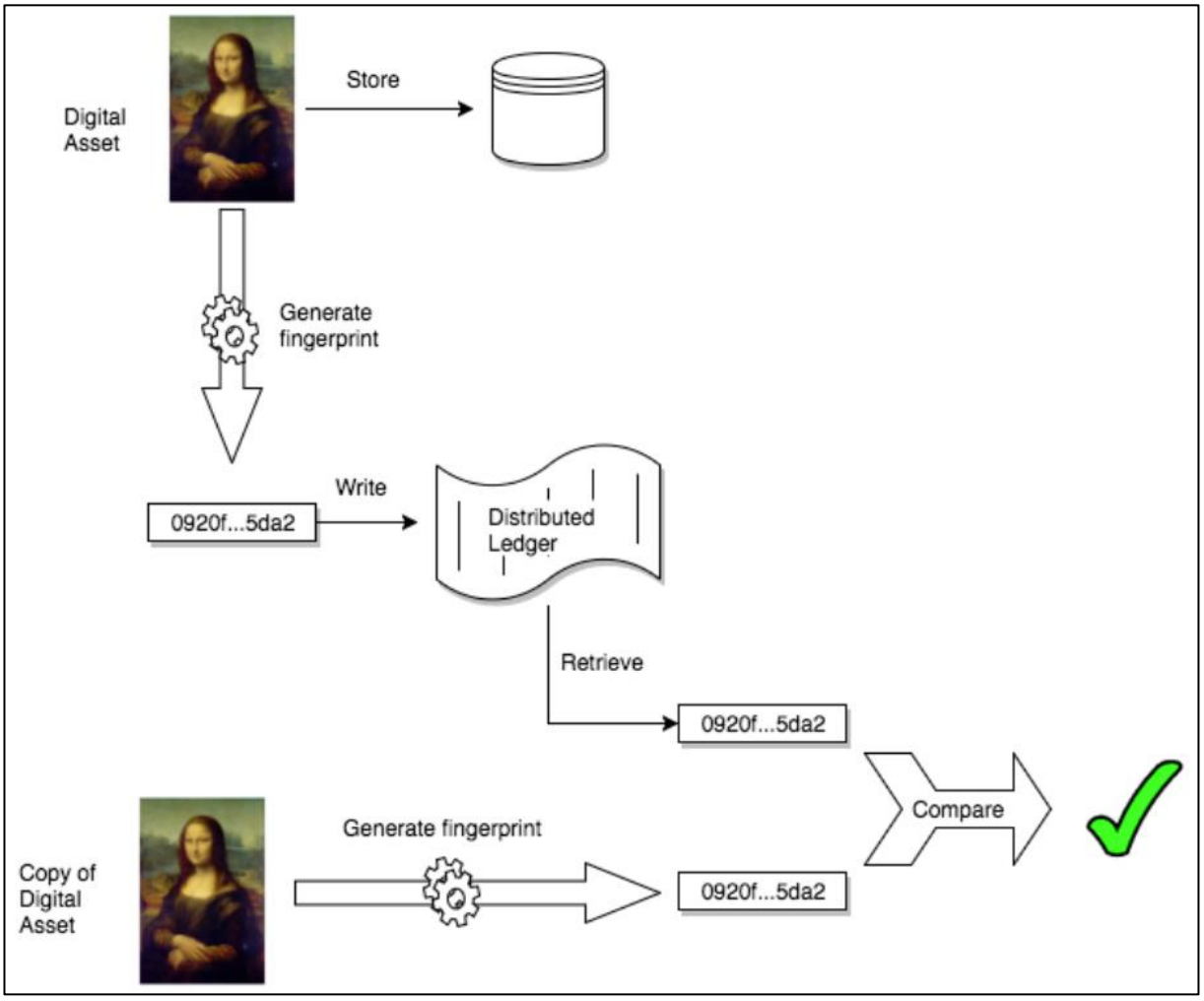
Quite a few people have been in touch with the idea to have evidential integrity be protected by a blockchain's tamper-resistive measures. Having the ability to store records of electronic material and having that storage hold the context of its creation is a clear benefit. This section looks through the methods and literature regarding how organisations and people have expressed their thoughts and creativity to come with solutions to protect data integrity with the assistance of blockchain technology.

Different posts and articles have been suggesting a combination of the chain of custody and blockchain to make it immutable. Calvin Liu (2017) writes that the capabilities of a merge could potentially create a tamper proof access to evidence. The evidence would need to be encrypted and have the blockchain capabilities added on to it. This encrypted data would only be accessible via a software which is custom made for this purpose. Access would then be granted through encryption keys and note data such as time, date, and possibly the user ID of the party accessing the chain and add this data to the unalterable records for the data set. The blockchain itself could be read through functions similar to Bitcoin which allows for the ability to examine the historical records without necessarily be able to access the data itself.

In a hypothetical experiment to secure video footage carried around by police officers on duty, Davidson (2017) brings up the idea of utilising blockchain to preserve the hash value of the video clips. All the data needs to be stored, managed, catalogued, and retrievable, but all the video editing software available today, maintaining trust in the integrity of the video clip itself can be challenging. The proposed process begins with the police officers arriving at the station after their shift and plugging in the camera to a device to split up the footage to ten-minute chunks which is then uploaded to secure cloud storage. The functionality of this service will start by providing storage and controlled access, record metadata about each clip (such as recording device, where and when, etc.), compute a hash of the clip and the metadata, and finally put the hash of the video and the hash of the metadata onto the blockchain. This blockchain would then be readable by anyone but only writable by the police. If any clip were to be needed in court it could be verified using the corresponding hash stored in the blockchain and compare it to a newly computed hash made of the same hash-algorithm.

U.K. Ministry of Justice's technical overview by David Salgado (2016) regarding the potential application of distributed ledger technology, provide additional insight and states limitations to its integration with chain of custody. A distributed ledger using digital fingerprints in an investigation process would normally consist of images duplicated off the original because several people would be working the same case. Illustrated below is how its functionality would look like in a probable real-life scenario (figure 2).

Figure 2



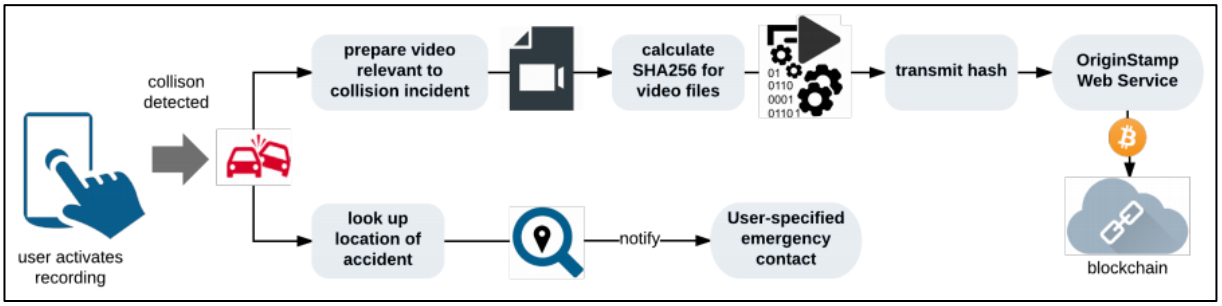
A functional implementation will show for a series of properties pertaining to the hash value stored in the chain. The blockchain would provide; immutability (append only and tamper proof), timestamping, resilience (every node in the network has its own accurate copy of the ledger), transparency (anything written in the blockchain, usually just the digital fingerprint, is readable by anyone), and distributed trust.

Further use of the chain stated in the report include split video evidence hash and digitally signing transactions. A large video clip can be divided into smaller clips where each one is hashed and to further compute a hash made of all the other hashes. If a clip is missing or out of order it will show when the hash could not be reproduced due to lacking input. The digital signature of transactions would be used when evidence is transferred to another party to provide documentation and context to the chain of custody. This way we can prove that the evidence was singed for and in order when provided to the next party, and any issues with the integrity of the digital evidence later on is not caused by the previous party, avoiding internal disputes. However, there are some issues that the blockchain by itself cannot solve for. Salgado points to the fact that the evidence integrity cannot be protected before it is collected and entered onto the blockchain. This allows for alterations before such time by anyone who may have access to it beforehand. The hash value only accounts for the time of computation after acquisition by the authorities. Digital fingerprints in the blockchain neither accounts for destruction of the actual corresponding physical evidence in the evidence lockers. Therefore, a quick incident response is important as well as physical storage of the digital evidence.

The issue of alteration before acquisition may be solved in a particular case regarding video evidence in a conference paper by Bela Gipp, Jagrut Kosti, and Corinna Breitinger (2016). Their

paper suggests the use of a Bitcoin blockchain to secure and verify the integrity of video files, but their paper also include a precautionary step in their suggested technology to secure the video file integrity before it is collected by proper authorities. By utilising an android phone and developing an application using the phone's sensors, they are creating a dashboard camera for vehicles with the added functionality of computing hash and transmit this value to a decentralised trusted timestamp service and further to a blockchain network (figure 3).

Figure 3

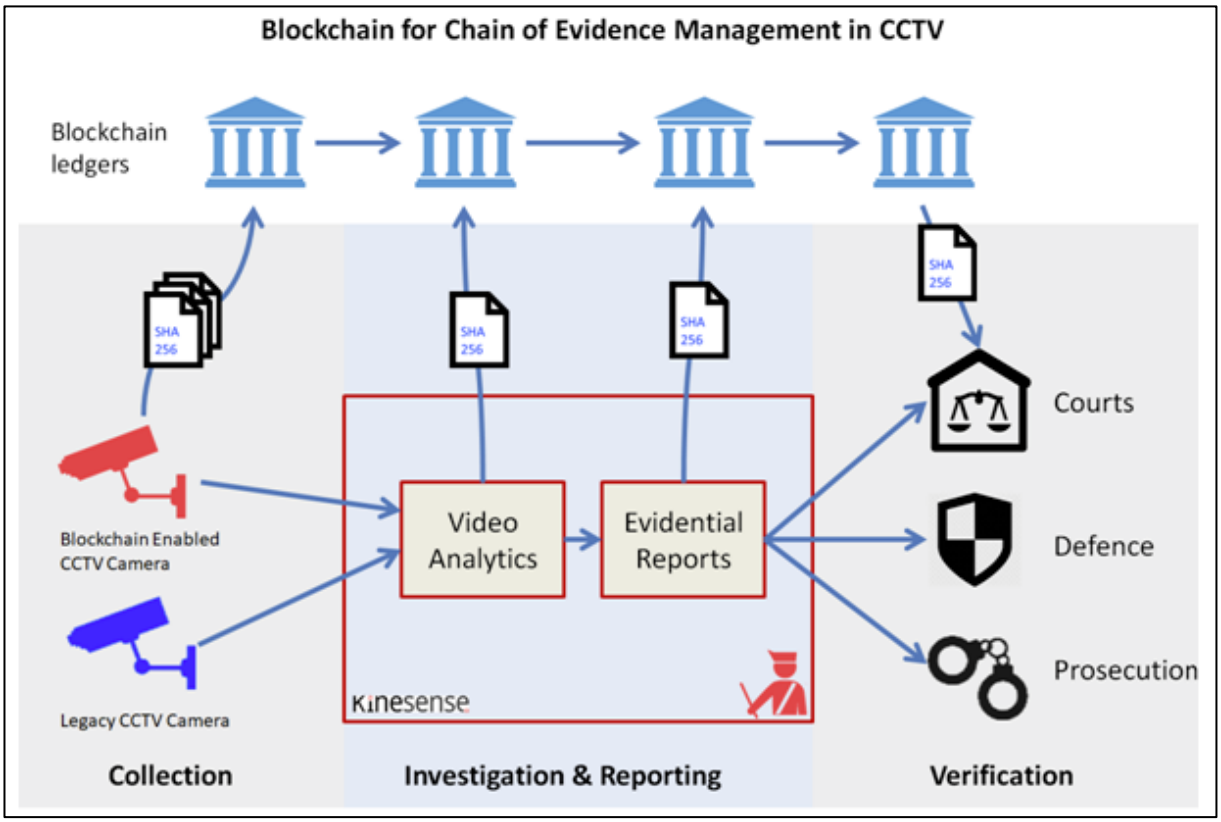


The functionality rests in the technology available to the phone. It starts by continuously record video in chunks of ten seconds where no more than two chunks are present at any time of recording. Until a program defined collision or accident has occurred, the oldest ten second chunk is continuously overwritten, and a new recording starts, keeping the recording in a twenty second loop. If an accident occurs a third ten second chunk is starting to record before the video cuts off and the application proceeds to the next step. The car accident is triggered using the phone's build in accelerometer to detect an impact. The x, y, and z axis are queried every hundred milliseconds and will react to any significant sudden change in values. Implementation of GPS coordinates lets the program account for error handling as well by checking for movement after occurrence. Significant movement after a program registered collision occurs results in no collision being declared. When the program has recorded the full thirty seconds (twenty before and ten additional after), the application merges the video files and computes a SHA256 hash value of the collected video files. This value is then sent to the trusted timestamp service and stored on the blockchain for integrity protection. As this goes on, the accident is being located and any emergency contact listed by the user are contacted. The video file on the phone can be verified to remove doubts of alterations by comparing the video file's hash with the one stored on the blockchain network through the distributed trusted timestamp services. All actions of hashing and transmitting the values are done in the background of the software (not available to the user), making it impossible for the user to intervene in the process. The program also includes the option of immediate save and timestamping of videos. This may come in handy when in experiencing irregular events. Answering to the previous issue in regard to proving the evidence integrity before it has been collected by authorities, this solution is promising in the case of video evidence and may hold further implementation yet to be discovered. As stated in their paper (Gipp et al., 2016, p. 9), tamper proof video evidence can be used in areas such as; video surveillance, automated timestamp of important meetings, footage to prove priority or copyright creative ideas, military aircraft or drones, and body cameras worn by police and law enforcement.

Kinesense is a company that provides software solutions for video investigations. Their products such as video analysis, clarification, face detection and recognition, and other forensic video services will enable practitioners to select analysis methods, validate results and quickly report discoveries with ease (Doyle, 2018). The video analysis tools are designed to preserve the chain of custody from capture to court and complies with the ISO 17025 for evidence management. The features described include hashing of video frames and recorded user actions. This information is then available at every stage of the video analysis process and allows for a printout disclosing all steps undertaken in a detailed report. Kinesense is working on developing a chain of custody concept based on blockchain. Their video platform is already in use by some police forces and it already include hashing as a part of the technology, which may be used to

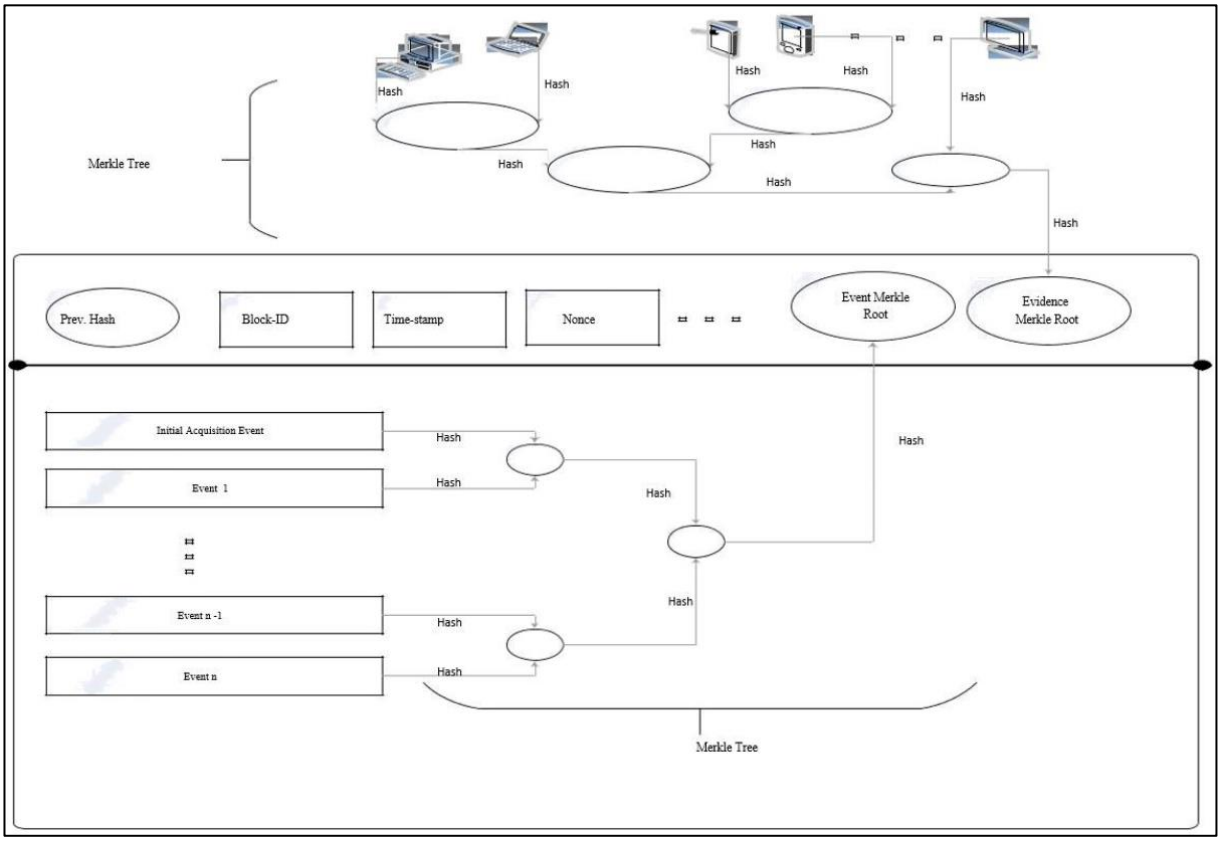
confirm authenticity and prove the chain of custody (Sugrue, 2018). Mark Sugrue writes that when evidence video is collected from the source (such as a CCTV/ surveillance camera), the digital signatures are generated and stored in a system acting as the blockchain ledger (figure 4). He also points out that the camera device itself could carry out this step, providing integrity protection to all recorded footage.

Figure 4



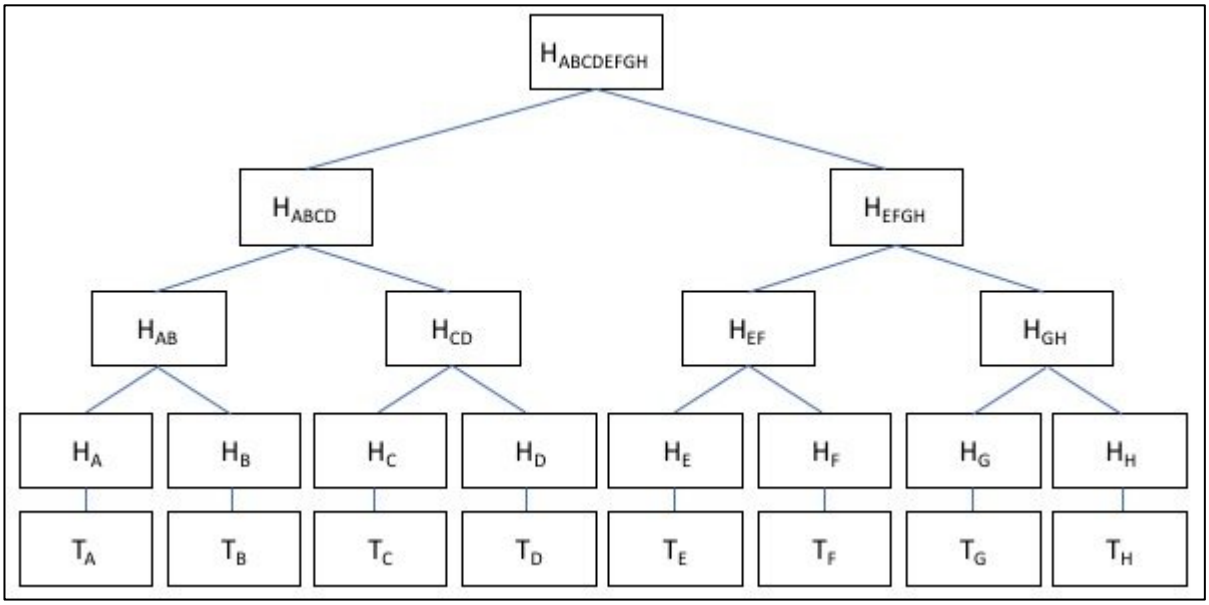
A short research paper by Auqib Hamid Lone and Roohie Naaz Mir (2017) issued in a cyber security journal goes a little more in depth than we have seen so far. The paper show insight into the possible implementation of a practical blockchain solution. The evidence we wish to preserve is first encrypted and then gets included to the blockchain with access only by desired parties while access data (such as time, date, and user ID) simultaneously is recorded to the chain through "smart contracts". Smart contracts are computer coded contracts operating in the blockchain. These contracts can automatically verify, execute, and enforce the contract based on the terms coded into the contract. If the conditions of the contract are met, payments or value are exchanged based on the contents of the contract (Gates, 2017, pp. 72–73). Smart contracts have been gaining popularity the last few years, especially since Ethereum made programming them a basic tenet of their blockchain's capabilities (Mougayar, 2016, p. 41). Having data encrypted allows for access to the historical aspect of the chain for examination without an open data view, similar to the suggested method of Liu (2017). The "Forensic-chain" model proposed (Lone & Mir, 2017) is based on an Ethereum blockchain, allowing users to write smart contracts and transact with predefined rules (Hertig, 2017). The "genesis block" consists of block-ID, timestamp, location of acquisition, and other relevant information in additional to a hash "merkle root" of the events taken place and a hash merkle root of the evidence (figure 5). Subsequent access and actions are recorded which produces new blocks, including the same properties and attributes, with the addition of the previous block's hash included and the evidence merkle hash excluded. The genesis block is the very first block on a blockchain and have no previous block before it (Gates, 2017, p. 108).

Figure 5



Merkle trees originates from Ralph Merkle in a paper from 1987 (Floyd, 2017) based on encryption and digital signatures. The merkle tree structure takes a number of hashes and represent them with a single hash. This is an efficient method of mapping data and allow easy identification if any changes has occurred (Curran, 2018). If an attempt to tamper with any piece of the data in the hash tree has occurred, it can easily be detected by remembering the hash pointer on the top (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016, p. 13). As illustrated below (figure 6), the lower part consists of transactions while the middle consists of represented hashes leading up to the single value at the top. The single value at the top is referred to as the root, the middle as the branches, and the bottom as the leaves of the tree (Floyd, 2017). This structure is continuously pairing and hashing values until it reaches a single hash value.

Figure 6



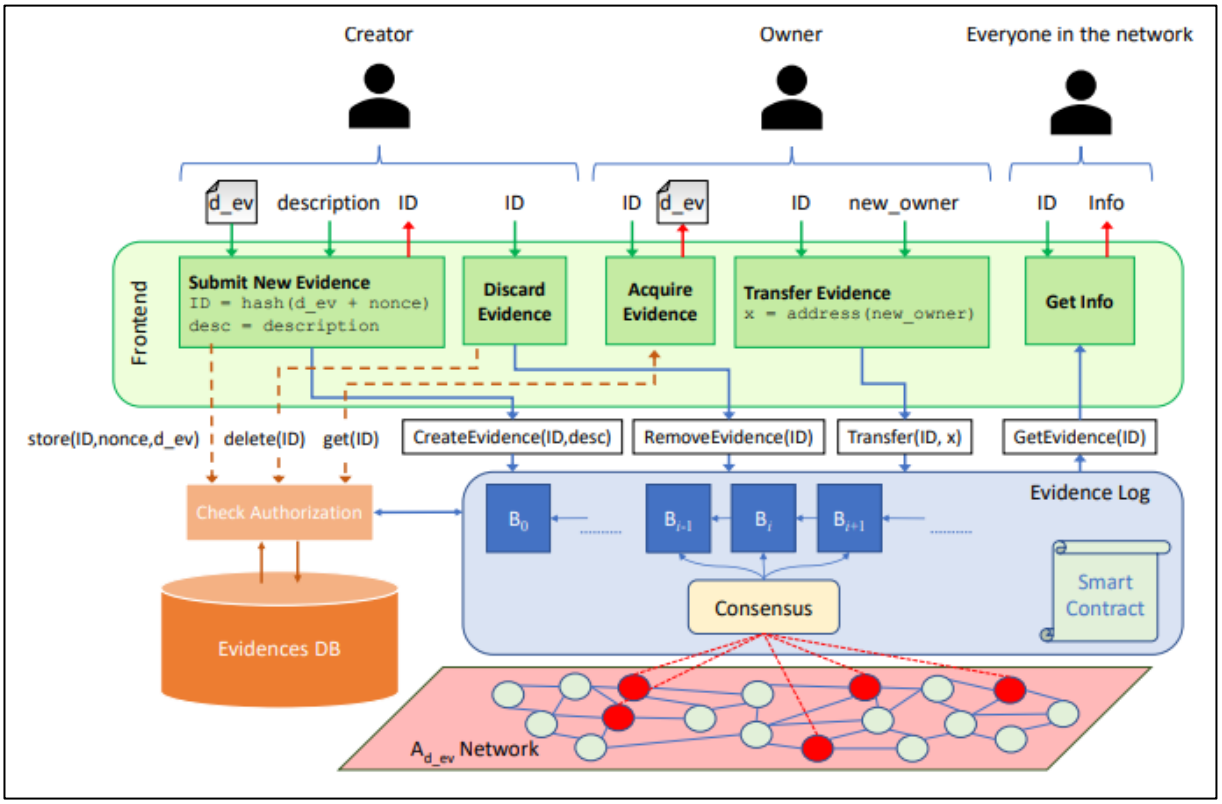
The "Forensic-chain" model described (Lone & Mir, 2017) have several benefits applicable to forensic applications. Integrity maintenance, transparency, authenticity, security, and auditability pertaining the digital evidence are desirable functionality available through these methods. Other areas it might show use can be fraud reduction (record transparency), event or action verification towards evidence, and cost reduction in the means of no longer be in need of a trusted third party to verify evidence.

A technical whitepaper of the Evident-Proof services (Boness, 2017) issued by Berkshire Cloud has a different approach to utilising blockchain for integrity purposes. The whitepaper states that the service is based on blockchain, Ethereum, and tokens to turn data into immutable proof of evidence chains (Evident-Proof, 2017, p. 5). Although more complexity is involved, the basic functionality is described with users, software, service, and requests in the technical paper (Boness, 2017, p. 6). In this case the user of the service is an organisation joining the service agreement. Evidence data is fed to the software and cryptographic digests (hash values, but referred to as "seals" in the paper) are computed from this data. The verification is done while it is still in the software and dispatched as a bundle of seals including metadata to a central platform where mirrored storage occurs using two separate blockchains; one private and one public. The bundle is split for individual storage on the private blockchain and batched storage on the public blockchain. When confirmation is received from both blockchains, a receipt is issued to the user to be used when making requests to access the evidence. There is a one-to-one relation between seals and receipts, meaning there are only one receipt for each seal. When in need to verify evidence, a certificate request is made, including the evidence records to be proved plus a list of receipts to the seals for those records. Copies of the seals will then be fetched by the system form the private blockchain and the requested certificate verifies that the contents of the evidence are in properly intact and in timely order. If evidence is missing in the comparison, then the requested certificate will indicate such omissions. If a third party wish to verify evidence themselves, they can with permission from the original user by issuing a request on their own. This request, however, obtains records from the public blockchain instead of the private one. By doing so, the two separate blockchains will provide assurance of the certificate integrity beyond the standard of any one blockchain. The two set of independent miners for the private and public chain works separately to verify the integrity of each blockchain.

Silvia Bonomi, Marco Casini, and Claudio Ciccotelli (2018) developed a prototype for a Ethereum based blockchain chain of custody and published a research paper on its performance. This blockchain is developed for a private network and utilise the "proof of authority" (PoA) instead of "proof of work" (PoW). PoW is the original consensus algorithm used in a Bitcoin

blockchain networks (Tar, 2018). It is used to confirm transactions and produce blocks to the blockchain by having miners compete against each other, usually with a difficult mathematical puzzle which is complicated to solve, but easy to verify (e.g. hash function, integer factorisation). However, the puzzle should not be too complicated, as the transactions will need to be executed after a short period of time. This solution protects the networks from malicious attacks such as denial of service (DoS), where someone is attempting to render the network unusable for a period of time by exploiting vulnerabilities (Mitchell, 2018). PoA on the other hand is an alternative consensus mechanism where specific nodes are allowed to validate blocks. This is done by having the validator's identity in the network being at stake, voluntarily disclosing who they are in exchange for the right to validate blocks (POA Network, 2017). PoW is mostly suited for public networks while PoA is a suitable substitute for private networks (Bonomi et al., 2018, p. 3). The research paper of Bonomi et al. also utilises Ethereum blockchain and smart contracts for their developed solution. They provide a fair overview of how the implementation works and the functionality behind to support it. Their model for the blockchain chain of custody architecture (figure 7) has three main components: the frontend interface handling the users, the database for evidence, and the evidence log.

Figure 7



This model has several functionalities spread across the components (Bonomi et al., 2018, pp. 6–7). The frontend runs a local instance on each node and connects to the database and the evidence log when access is needed. The network allows different entities various permissions depending on their role in the system. People may create, remove, transfer, or view evidential information via the frontend interface that is available. The database and/ or file repository has ordinary general functionality meaning it stores the evidence along with its identifiable information. It is distributed, managed by authorised entities, and access is only permitted if the requesting entity is authorised according to its role. The evidence log is based on blockchain and stores information about the evidence and the events it undertakes. It stores information such as the evidence ID, description, identity of the submitter, and the history of ownership (transfers) including timestamps. The blockchain network in this case consists of two kinds of nodes; validators and lightweights. The validator's three functions are: storing a copy of the blockchain, validating transactions, and participate to the work in the consensus protocol. The

lightweight nodes for the simple purpose of issuing transactions and relies on the validators' functionality. The blockchain implementation is done through "Geth", an interface allowing for Ethereum node implementation including private network setup and configuration of the blockchain and consensus protocol (Bonomi et al., 2018, pp. 7–8). The developed prototype was concluded to be functional and show support for the chain of custody process with reliable performance.

3.3 Literature summary

Starting with the approaches to integrity preservation, several methods were explored and discussed individually and compared to different versions. The important techniques to take away from this section is the write-blocker, imaging, hash functions, digital signature, timestamp, encryption, and the chain of custody. These techniques are most commonly used to protect data and information and have a high probability of inclusion in developing a strategy to be used for integrity preservation and further be integrated with a blockchain. The cryptographic hash functions mentioned in the tables (Ćosić & Bača, 2010a; Hosmer, 2002) shows the history and version of hash that has been used over time. The less secure hash functions, such as the mentioned MD2, are no longer used to the same extent due to the replacement of the new functions with higher standard of security. The suggested digital evidence management framework (DEMF) is also an interesting approach including GPS location aspect of the proposed function (Ćosić & Bača, 2010b).

The blockchain variations explored for integrity purposes include a great number of points to be further discussed. First thing to notice is the type of information that is selected to be stored when the blockchain is used as a chain of custody (excluding previous block hash). In theory this can be any kind of information, but some attributes are generally included as the base. Such attributes may include time, date, user ID, and hash value(s). Further information may include nonce, a description, identity of the original creator of the log, and identity of the entity currently in possession of the evidence (Bonomi et al., 2018). Nonce is an input made from cryptographic methods with the property of allowing a value to only occur once in a given context. Using a random number generator is one possibility to do so, but will require an extensive length of the nonce to avoid collisions (Zenner, 2009, pp. 1–2). Even though blockchain contents usually are made open for inspection by anyone, some of the mentioned solutions suggests to encrypt parts of the data contents on it for evidence protection (Liu, 2017; Lone & Mir, 2017). This is for the different purposes of accessing and examining historical data, and the access to read and interpret the actual data itself.

From the projects and services described using blockchain, there are three utilising the Ethereum blockchain model (Bonomi et al., 2018; Evident-Proof, 2017; Lone & Mir, 2017) and one using the Bitcoin blockchain (Gipp et al., 2016). The different models allow for various capabilities suited for their individual purposes. This also counts for the consideration discussed regarding the use of PoA over PoW for the blockchain (Bonomi et al., 2018). These methods differ in the use of computational power needed for PoW opposed to the authorised entity for PoA.

Out of the explored blockchain services and solutions, four is purposely developed for video (Doyle, 2018; Gipp et al., 2016; Sugrue, 2018) or discusses video files (Davidson, 2017; Salgado, 2016) while the last four are focused on discussing solution for general evidence files (Liu, 2017; Lone & Mir, 2017) and developing services for it (Boness, 2017; Bonomi et al., 2018; Evident-Proof, 2017).

Evident-Proof (Boness, 2017; Evident-Proof, 2017) is the only one of these services or projects taking advantage of the concept of using two blockchains in their strategy. The benefits of this approach are the separation of access for the original owner of the evidence and third parties granted access upon request with permission. It also allows for independent sets of miners divided on the private and the public blockchain.

3.4 Literature conclusion

There are a lot of interesting approaches and strategies explored in the integrity- and blockchain solutions discussed in the previous sections. The methods and techniques carried over to the summary section includes the most essential methods necessary to develop a proper evaluation of the significance blockchain technology may have on preserving the integrity of electronic evidence.

The integrity protection section has methods relevant and applicable to evidence preservation, but no all the solutions are explored to the appropriate depth to make a decisive approach. A few of the mentioned methods need no further explanation, but some, including the hash functions, encryption, and imaging techniques needs to be discussed further and be set up for comparison for a deeper analysis. This will allow for a more objective and thorough consideration instead of deciding based on the solutions and systems discussed in the previous sections.

For the blockchain section, most of the discussed solutions are within the same field as the current project. It makes of little difference if they only handle video files because they store the hash value of the given clip in the blockchain, which is just a string of data as the same with any other type of hashed evidence files. The solutions include a lot of valuable information regarding blockchain and evidence integrity, but none of them seemed to have developed their own base for the blockchain. As the summary states, three are using chains based on Ethereum and one based on a Bitcoin chain, whereas the other solutions simply discusses the topic of blockchain in general. A lot of the techniques and capabilities looks interesting and promising. Basing the conclusion on the blockchains in the discussed solutions, it would seem as the best decision would be to do a deeper analysis of the blockchain's requirements and combine functionality. A blockchain for the evidence purposes in the context of this project would be recommended to be developed internally within an organisation, preventing it from being dependent on the technologies found in existing blockchain solutions (such as Ethereum or Bitcoin).

CHAPTER 4: METHODOLOGY

Search strategy:
The topics covered in this project can be split into several research areas. The main areas to cover include blockchain, digital forensics, digital evidence management, and digital evidence integrity preservation. There are multiple sub-areas within each of these fields which uncover additional subjects related to the fields to be further explored. The purpose of the research was to find information to assist in the overall goal of the project, providing arguments for or against solutions and finding answers to the aims and objectives of the report. Searching through different sources was carried out with the intent of supporting or disproving statements and methods considered to have effect on the overall project.

Data collection methods:
Articles, books, interviews, journals, proceedings, and technical reports.

Resource search criteria:
Includes the following key areas and in combination with other words for more accurate results when searching for a specific subject.

- "Blockchain technology"
- "Digital forensics"
- "Digital evidence management"
- "Digital evidence integrity preservation"

Inclusion criteria:
For any resource to be included in this report, it must contain relevant information and be credible. Articles and documents with anonymous author and unknown origin would normally not be considered a trusted source and therefore rejected from inclusion. Allowed sources would contain well written and relevant contents pointing to a creditable author or trusted organisation.

Content evaluation criteria:
The resources must be additionally evaluated on their contents to ensure quality and applicability to the research area. Contents in relation to this project are considered based on accuracy, objectivity, coverage, and its relevance to the subject in question.

Research limitations:
Research material is mostly of recent years due to the topic being relatively new. Most of the sources which directly correlates with the topic are found online in reports, services, and papers. Additional sources are also used, but they cover the topic separately by containing information on either blockchain or digital forensics.

CHAPTER 5: REQUIREMENTS AND ANALYSIS

There are several key areas to consider in this chapter. A further analysis must be made to address the required functionality and optimal outcome of the blockchain. Simply putting all the discussed variables together would render the solution insufficient, leaving it unacceptably incomplete. This chapter will dig deeper into the methods and options available to single out the best ones based on objective reasoning.

5.1 Type of blockchain

The first consideration is the type of blockchain to use for our purpose. Previously discussed solutions vary in the use of public and private chains for different reasons. Even though labelled separately, they do share the similar basic functionality of; decentralisation in a peer-to-peer network, maintaining replicas through consensus protocol, and providing immutability to the ledger (Jayachandran, 2017). The main difference in public versus private blockchains lies in the access rights. Anyone can take part and participate in a public blockchain as there is no access rights. All participants can join, leave, read, write, and audit the chain to the extent of its programmed capabilities and be a part of the consensus. A private blockchain would be the exact opposite, as participation, read, and write privileges are not given unless permitted by the ones with authority to do so (Khatwani, 2018a). Although a public chain will allow for more transparency (Parker, 2016) and a way to protect the users from the developers (Buterin, 2015), a private chain will in most cases allow for faster transactions, network of trusted nodes, permission table, and more control over rules and protocols of the application (Buterin, 2015; Parker, 2016). In the context of this project, the choice of implementation should be a blockchain allowing for private use in an organisation setting. Plenty of functionality comes with using existing blockchain platform such as Ethereum, Stellar, Ripple, and other variations, but complete flexibility and control is met by building and developing a custom blockchain. It might be easier to access a complete platform whereas the user can set every aspect that is available, but such solutions usually also comes with trade-offs between decentralisation, scalability, and security (Shilov, 2018). Development of a custom blockchain allows for own choice of programming language, control of code base, ability to manipulate updates, and other functional choices.

5.2 Consensus mechanism

A clear comparison of valid consensus mechanisms must be made before any blockchain can be implemented to a network of nodes. The three algorithms in question are the Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Authority (PoA).

Starting with the original Bitcoin consensus (Tar, 2018), PoW makes the participating nodes compete against each other in a process called mining, racing to be to first to solve a mathematical computation. The miners on the network adds pending transactions in the network to the "block" and tries to solve for the mathematical problem to find a certain resulting hash output based on the contents of the block (Jimi S., 2018b). A resulting hash beginning with a certain number of zeros is commonly used. The first node to find this hash value may broadcast it to the other nodes (as proof of work) for verification and will upon confirmation and consensus between the majority of nodes, be added to the blockchain (Jimi S., 2018b). This consensus requires high amounts of computational power and can be regulated depending on the size of the user base in the network (Tar, 2018).

PoS on the other hand is not about mining, but validation. The next node in the network responsible for the creating the block is determined by the PoS algorithm. In a PoS system, the validators each own some stake in the network as collateral to vouch the block. The participants in a PoS network trust the chain with the highest collateral (Naumoff, 2017). The PoS algorithm was created to solve problems with the existing PoW algorithms. The decisions are based on multiple factors to make it work. The size of the stake and the interest of validators are taken into account, the time of which the validator had its previous decision agreed upon by the network participants, and whether the outcome of that decision were met with approval by the majority of the network participants (Naumoff, 2017). The last consensus is the PoA, which as previously explained, is voluntarily disclosing the validator's identity as stake in the network in

exchange to have the right to validate blocks (POA Network, 2017). The PoA consensus mechanism is a modified form of the PoS, explicitly allowing certain selected nodes to validate blocks. When the identity and reputation of validators is at stake it creates an incentive where acting in the interest of the network and keeping it secure becomes the priority and the best course of action to take for a validator (POA Network, 2017).

The purpose of this report revolves around the topic of evidence items, and is generally aimed at an organisational setting, not a large anonymous decentralised group of casual entities. The choice of deciding on a consensus mechanism in this context in leaning toward the PoA consensus. This will allow for authorised validation of blocks and permission of participants on the network, preventing nodes from freely accessing the network. A PoA would also benefit in the sense of the lesser size of the blockchain network (compared to other large chains such as Bitcoin and Ethereum), PoW would be less effective to secure the network because it would be easier to control the majority of the networks computational power (Bonomi et al., 2018, p. 3).

5.2.1 51% attack

If a miner in a network control the majority of the computational power, it can effectively find the solution to the mathematical problem faster than the combined effort of all the other nodes on the network. If this happens it can allow for a network attack referred to as a 51% attack, a case when a user or a group of user control the majority of the mining power (Tar, 2018). A malicious miner can then create a separate fork in the blockchain and later take control of the network. A PoW blockchain consensus validates the longest chain as the "true chain" meaning the corrupted chain becomes the true chain and can allow for the corrupted miner to gain control (Jimi S., 2018a). A 51% attack may allow the corrupted miner to select transactions to be included in blocks and cause the issue of "double spending", where the same currency is spent twice (Khatwani, 2018c).

5.2.2 GDPR: Right to be forgotten or erased

One crucial setting any blockchain implementation needs to consider is the relatively recent reform on data protection of May 2018 called the General Data Protection Regulation (GDPR). The GDPR requirements apply to each member state of the European Union and has its goal set to protect consumer and personal data across EU nations (Lord, 2018). Non-compliance of the regulation may have substantial consequences, especially in the form of administrative fines. Article 83 paragraph 5 & 6 of the regulation states that infringements or non-compliance shall be subject of administrative fines up to €20 million or 4% of the total worldwide annual turnover, whichever is higher (The European Parlament and the Council of the European Union, 2016, l. 119/83). This is important information to remember in regard to developments and use of blockchains. Article 17 of the regulation mentions the "right to erasure", also known as the "right to be forgotten". Paragraph 1 of this article states the rights of a data subject to have all personal data of him or her to be erased without undue delay (The European Parlament and the Council of the European Union, 2016, l. 119/43). One of the core functionalities of the blockchain is the immutability aspect to ensure that no data can be altered. Because of this it will be of outmost importance to not store any personal information in the blockchain, but use other techniques to identify or refer to individuals.

5.3 Image techniques

Investigators should choose imaging tools that have been accepted by the forensics community and is efficient in both speed and compression. Marjie Britz (2013, p. 286) writes that images are recommended to be written to a raw data format. These images have longevity, transferability, and, unlike proprietary image formats, raw formats can be accessed and interpreted by all popular forensics packages and does not have any backward compatibility issues. However, raw images are not compressed and can be quite large, even if it contains little data. It is a sector-for-sector copy and cannot store metadata such as drive serial number, dates, or information about the investigator who performed the acquisition (Garfinkel, Malan, Dubec, Stevens, & Pham, 2006, pp. 17–18). Although it does not contain this data in the image file, software tools used to create the image often include a separate file containing metadata about the image such as timestamp, name of the software used, and cryptographic hash used for later verification (Vandeven, 2014, p. 35). A forensics suite called EnCase have created another file

format called the “Evidence File” format, using the extension E01, and is based on the Expert Witness Format. E01 files have both a header and a footer containing metadata, and is compressed by default. A Cyclical Redundancy Check (CRC) is additionally included in E01 files at block intervals, which provides integrity checks to the blocks of data, similar to a cryptographic hash provides integrity check to an entire image (Vandeven, 2014, pp. 8–9). Other image formats are available as well, but these two are the most wide-spread and used. For this project, all images are meant to be evidence files which means they are expected to be subjected to evidence examination and analysis. Most evidence data examinations take place in a setting utilising forensics software, tool, suits, or applications of some sort, normally supporting both image file formats. This project will proceed with the selection of the E01 format based on the above discussion of their capabilities. The E01 is the evidence file format and may include more feature and characteristics which may be necessary in digital forensics setting.

5.4 Hash function and collision

The hash technique to use is next in question. Hashing is normally used in two ways; hiding the original contents of a message (e.g. a password) or to check the integrity of data (Buchanan, 2017, p. 63). Different hash variations and methods are discussed previously but have not been put against one another for comparison. A reason for switching to a more secure hash algorithm would be if there were an issue of hash collisions or doubt in current algorithms security. A collision is when two different inputs has the same hash value as output, e.g. when h(m1) = h(m2). Hash functions is never completely free from collisions. There is an (technically) infinite number of possible input values and only a finite number of possible output values (Ferguson & Schneier, 2003, pp. 84–85). The secure hash algorithm (SHA) is a family of related cryptographic hash functions (Newman, 2007, p. 124), as illustrated in the tables previously. The older SHA-1 and MD5 algorithms are currently in wide use, but flaws have been found in both and should retire in favour of more secure hash (Kenan, 2005, pp. 22–23). Smaller range of outcome makes probability of collisions between hash higher. A larger bit hash can therefore provide more security because of the increase in possible combinations. As the tables illustrate, MD5 is a 128-bit hash, which is below most of the outputs the SHA family can produce. SHA-1 is a 160-bit hash and SHA-2 has an own set of hashes and comes in a variety of lengths, with the most popular one being 256-bit (Lynch, 2017). NIST have already approved a replacement cryptographic hash algorithm called SHA-3. It does not share the same mathematical properties as its predecessors and should be more resistant to cryptographic attacks, although it might take some time before a wide spread implementation. Moving to SHA-3 now will probably lead to having cryptographic-relying applications and devices error out, because they cannot recognise the digital certificate. Migration to SHA-3 will happened when SHA-2 starts to get weakened (Grimes, 2017). This project needs a hash that is safe its day and age. Any choice made today will have its cryptographic security broken in the future when time and technologic advancement moves on. The safest selection today would be the SHA-256, which is also the most popular in terms of security versus functionality, and it is the same hash function as the Bitcoin’s blockchain use for its PoW algorithm (Khatwani, 2018b). The hash has more than just a forensic value, its works as a deterrent. Knowing that hash is used may deter possible intruders from even considering tampering with the digital evidence (Stone, 2015).

5.5 Encryption and digital signature

Encryption may be used for a couple of functionalities besides hashing images of evidence and blocks in the blockchain. Similar to the solutions for blockchain integrity by Lone, Mir (2017), and Liu (2017), that were discussed previously, encryption techniques may be used to secure blockchain contents while keeping it open for examination. Evident-Proof, also previously discussed, reach the same result by having two blockchains implemented in their services, where one is private and the other one is public (Boness, 2017). What version is better is entirely up to the solution and what information that require protection. A decision will have to be made at a time it is clear what type of data that is being recorded onto the blockchain.

The primary goal of cryptography is the secrecy of plaintext from eavesdroppers and other unauthorised parties trying to get information about the text (Delfs & Knebl, 2002, p. 4). Digital

signatures can be implemented for the users of the blockchain when managing transactions as an additional layer of trust and certainty of the identity performing the action. Digital signatures are data strings which associates a digital message with some originating entity (Menezes et al., 1996, p. 426) and are supposed to be a digital equivalent of a handwritten signature on paper. There are two properties we desire from a digital signature that correspond well to a written analogy. First, only the original signer can produce the signature, but anyone who sees it can verify its validity. Secondly, the signature must be tied to a particular document so that the signature cannot be used to indicate the signature owner's agreement or endorsement of a different document (Narayanan et al., 2016, p. 15). As with the classical handwritten signature analogy, the intended purpose of digital signatures is to provide authentication and non-repudiation (Delfs & Knebl, 2002, p. 3) with the goal to simply verify the sender (Kenan, 2005, p. 22).

One of the most significant applications of digital signatures is the certification of public keys in large networks (Menezes et al., 1996, p. 425). Digital certificates are most commonly used for secure initialisation of SSL connection of web browsers and web servers, but are also used for sharing keys for public key encryption and digital signature authentication (Rouse, 2018). The majority of digital certificates are issued by a certificate authority as a trusted third party, but it is possible for other entities to create its own public key infrastructure (PKI) and issue its own digital certificates. This may be reasonable for organisations wants to maintain its own PKI and issue certificates for own internal usage (Rouse, 2018).

As discussed previously, public or asymmetric encryption, uses two different keys. One is used to encipher data and only the corresponding key can be used to decipher it. In practice, one is called the private key and should be protected from disclosure by the owner, and the other is called the public key and can be made freely available to anyone who wants to conduct transactions with the private key holder (Kruse II & Heiser, 2001, p. 91). The most widely used public key cryptography is the Rivers-Shamir-Adleman (RSA) that is embedded in the SSL/TLS protocol to provide secure communication over computer networks (Rouse, 2016). Its security derives from the computational difficulty of factoring large integers produced of two large prime numbers. A second favourable public key cryptography is the Elliptic Curve Cryptography (ECC). This encryption is based on elliptic curve theory and can create faster, smaller, and more efficient cryptographic keys. The properties are generated through an elliptic curve equation, which is significantly more difficult to compute than factoring numbers. Compared to RSA, the ECC key sizes can be smaller, yet deliver the equivalent security using lower computing power and battery usage (Rouse, 2016). For these reasons, ECC would be preferred as the public key cryptography in this project, and as it is still being used as the public key algorithm by Bitcoin, we can have confidence that the robustness provided can safeguard the knowledge of the private keys (Rykwalder, 2014).

The image hash that is to be stored in the blockchain would be signed by the person performing the action or transaction in the blockchain. Hash functions are used in conjunction with digital signatures where the hash value, as a representative of the message, is signed in place of the original message (Menezes et al., 1996, p. 321). The digital signature is generated by encrypting the cryptographic one-way hash with the signer's private key. This way, the signature incorporates the encrypted hash, which can only be authenticated using the sender's public key to decrypt the signature. After decryption it is possible to run the same hash algorithm on the original contents and compare it to the hash that was signed for verification (Rouse, 2018).

The blockchain may utilise digital signatures as a replacement for sharing individual's identity. The reasons for this are for the verification of the sender/ transmitter, and the GDPR for storing personal information. A digital signature certificate may be issued by the organisation implementing the blockchain solution, having a database (not blockchain) reference to the person which may be subjected and removed if needed under the GDPR's right to be forgotten (The European Parlament and the Council of the European Union, 2016).

5.6 Additional considerations – physical storage and electronic tags

Even if blockchain may provide security for the evidential integrity, the physical aspect of the equation is still yet to be discussed. Before we can prove that the presented evidential data has maintained its integrity, we must prove that we maintained the integrity of the hardware that contains the data (Solomon et al., 2011, p. 85). Having the original physical evidence (e.g. disk drive, phone, storage media) lost, missing, or destroyed either deliberately or accidentally, may have consequences for the overall case. If the digital evidence cannot be properly recovered or reconstructed, it will be difficult proving that the evidence found are actually contents of the original media. On the page of securing the physical evidence, we also investigate the possibility of adding digital tags or barcodes to the evidence as an additional implementation to the functionalities of the blockchain.

5.6.1 Physical storage of digital evidence

After evidence have been collected at the scene, they should be transported to a forensics lab as a controlled environment to ensure security and integrity of the digital evidence (Nelson et al., 2015, p. 160). When handling computer components as evidence it is important to be cautious of environmental factors to avoid damaging the evidence. Static electricity, cold, heat, and humidity above a certain range can damage computer components and magnetic media (Nelson et al., 2015, p. 28), as well as factors such as direct sunlight, magnetic fields, oil, dirt, and dust. Related material should be placed singularly on appropriate shelving in a climate-controlled, dust-free environment (Britz, 2013, pp. 325–326). To avoid static electricity, antistatic bags should be used when collecting computer evidence (Nelson et al., 2015, p. 28). Besides keeping the technology safe from damage, it must also be protected because of its legal significance. It is important to provide additional security such as sealed containers and limited access to the storage area (Kruse II & Heiser, 2001, p. 12). The evidence storage containers/ lockers must be secured against unauthorised access using high-quality locks and limited key distribution alongside routinely inspection of the contents of the evidence storage containers (Nelson et al., 2015, p. 72). Anyone who takes possession of the evidence and the time of which they took and return possession must be documented along with the reason for possession in the first place. Defence attorneys will review records associated with the evidence and cross-reference it to other documents to find discrepancies that can be used to weaken the case against their client (Kruse II & Heiser, 2001, p. 8). These records are usually the chain of custody involving the evidence. If any link in the chain breaks, it will also break the integrity of the evidence. The court expects the chain of custody to be complete and clear of gaps, which is provided by demonstrating an evidence log that shows every access to the evidence, from initial collection to its appearance in court (Solomon et al., 2011, p. 65). The two easiest ways to render evidence inadmissible are to collect them illegally (e.g. no warrant) and to modify evidence after taking it in possession. Only personnel trained in proper handling of evidence and with understanding of the importance of maintaining the chain of custody should be allowed near evidence. The cost of training is less than the cost of losing evidence due to a single careless act (Solomon et al., 2011, pp. 71–73).

5.6.2 Electronic tags

There are several technologies used for electronic tags which may provide additional functionality for the solution discussed in this project. The tags being discussed in this section is in regard to the physical evidence and the evidence storage containers to semi-automate the process of the chain of custody. Digital tags and markers are used in many areas today, and people might not even realise it is there. Today, they are used in areas such as clothing and bottles (Catalyst, 2016), sports and race timing (RFID Race Timing Systems, 2017), animal identification, fuelling automation (Hidglobal, 2018), attendee tracking, library systems, logistics and supply chain, inventory tracking, and much more (Thrasher, 2013). The technologies covered in this section include radio frequency identification (RFID), near-field communication (NFC), and barcodes.

Barcodes are usually recognised as a small image of bars and spaces affixed to retail store items, ID cards, and postal mail to identify a product number, person, or location. The coded sequence of vertical bars and spaces represents numbers and symbols (Rouse, 2009). A barcode scanner

can record and translate barcodes from the image into recognisable alphanumeric digits, and send that information to a computer database, either via a wired connection or wirelessly depending on the model used (Schofield, 2015). Barcodes are often seen in supermarkets and retail stores, but they are also used to check out library books, take inventory in stores, and track manufacturing and shipping movement. There are several different barcode standards that serve different uses, e.g. the uniform product code (UPC) which is used for retail stores for sales and inventory, and the Bookland standard which is used for book covers, based on the ISBN numbers (Rouse, 2009). These linear barcodes can hold a few characters, but generally get physically longer when adding more data. It is typical by users to limit the barcodes to between 8 and 15 characters because of this increase. The scanners does not need direct contact with the barcode, but need to be within a range of 4 to 24 inches to scan. (Lowrysolutions, 2015).

Subsequent to the linear one-dimensional barcodes, we have the two-dimensional barcodes. These barcodes are often physically smaller in size than its linear predecessor (Holcomb, 2013), even though the patterns of squares, hexagons, dots, and other shapes allows its structure to hold up to 2000 characters (Lowrysolutions, 2015). The two-dimensional symbology comes from the necessity of capturing the entire width and length of the barcode to decode the data, compared to the linear version which only require the width. The two-dimensional barcode symbology varies depending on its use. The Aztec symbology is widely used by European airlines for online electronic ticketing and as a standard for electronic boarding passes on mobile devices, while the more common QR Code (quick response) is used to encode marketing URL's on different physical surfaces and is popular and easy to scan with smart phones and mobile devices (Holcomb, 2013). Even though both the one- and two-dimensional barcodes are useful low-cost methods to encode data track items, the type to select depends on application requirements, type and size of data, and the size of the asset or item (Lowrysolutions, 2015).

RFID technology on the other hand, overcomes certain limitations found in some barcode applications. Because it does not depend on optical technology like barcodes, no line of sight is required between the reader and the tagged object. Additionally, RFID transmits data wirelessly and have the properties of both read and write technology (Lehpamer, 2012, p. 1), giving it the capabilities to change, update, and lock data stored on RFID tags (Bonsor & Fenlon, 2007, p. 2). Generally, RFID represents a way of identification using radio waves. The RFID systems is composed of three components; RFID tag (transponder), RFID reader (transceiver), and the subsystem which processes and utilise the data obtained from the transceiver (Lehpamer, 2012, pp. 54–55). The three types of RFID tags are; active-, semi passive-, and passive tags. Active and semi passive tags use internal batteries to provide power, while the passive tags rely entirely on the reader component as a power source. The active tags will use its battery to broadcast radio waves to the reader and the semi passive tags will use the reader for broadcasting power. Active and semi passive tags can broadcast at a 30-meter distance, but can reach greater distance if provided with additional batteries to boost the range of the tag. Passive tags have a far lower production cost than active and semi passive tags and can read at a distance up to six meters (Bonsor & Fenlon, 2007, p. 4). The storage capacity of RFID depends on the type of tag, but is generally up to 2 kb. Simple RFID tags and cards are often used as ID, carrying only 96-bit or 128-bit serial number, or to store a variety of different item information for industrial applications (RFID Basics, 2016). It is necessary for predictable system performance when implementing RFID tags. Considerations may include tag and reader orientation, and environments that may involve phone signals, radio waves, electrical equipment, or other RFID readers (Lehpamer, 2012, p. 69). Another consideration is the data storage type to utilise. Data storage for RFID tags can be read-write, read-only, or WORM (write once, read many). Read-write can be both written to, overwritten, and have the data on the tag read at any time. Read-only cannot add or overwrite data on the tag, and only contain the data that were stored on creation. WORM can have data added to the tag once, but cannot overwrite data or add additional data thereafter (Bonsor & Fenlon, 2007, p. 4).

NFC is a method of communication, which can detect and enable technology in close proximity to communicate with no need for internet connection. This technology is evolved from RFID and operates as a wireless link, allowing small amounts of data to be transferred between devices a few centimetres apart (Faulkner, 2017). NFC are also found as small physical tags or

stickers, containing programmable NFC chips to provide any kind of information. They may contain information such as a link to a web address, but they may also be set to perform certain actions with a smartphone. This technology is advantageous to current QR (two-dimensional barcode) technology in the means that it does not require a scanner for communication where this information is immediately available on near proximity (Gordon, 2018). A range of devices may utilise the NFC standard and they are considered either passive or active. Passive NFC devices are tags and small transmitters which sends information to other devices with no need for a power source on their own, and cannot connect to other passive devices. Active NFC devices can both send and receive, and can communicate with one another as well as passive tags. The most common active device using NFC are smartphones, card readers, and touch payment terminals (Triggs, 2018). A wide range of NFC tags are available through a simple online search. Some tags include password protection and others may include encryption as protective measure. The storage size also varies by type, ranging from 32 bytes to 4 kb for regular consumer use cases (ShopNFC, 2018).

Evidence tagging may be an effective functionality addition to the already discussed implementation of the blockchain. As barcodes and electronic tags can contain informative data, we can use this capability to store information about the evidence and automate the chain of custody process. Automating the process using personnel identity (card, chip, etc.) and a digital evidence identifier, we can send the new chain of custody input straight into the blockchain, shortening the margin for human errors. Each time the evidence container is accessed, the chain of custody should log a timestamp together with the authorised person accessing the evidence (Nelson et al., 2015, p. 73). One of the limitations with linear barcodes is the amount of data it can store (Lehpamer, 2012, p. 51). While the two-dimensional barcode can store more characters, it will, along with the one-dimensional, require an optical scanner to get the information, making the option less attractive for an efficient and automated process. Considering the digital tags as a replacement, both the RFID and NFC each has their strengths and weaknesses. Even though NFC is a more recent technology, and RFID has been around for a while and is currently in widespread use around the world, they both employ radio signals for their purposes. NFC is a newer, more finely-honed version of RFID, operating at a maximum range of about 4 inches (Chandler, 2012). Because of the additional layer of security with NFC and proximity capabilities, this project will advance with NFC technology as electronic tag technology. There could be other possible use cases for RFID as well, but none of which we require at the moment. An RFID could potentially be used as an alarm tag on evidence, giving of a warning if it passes through the evidence storage gates (entrance/exit) without being scanned, or by having an RFID chip the size of a grain of rice implanted into the hand of the personnel as an access control implementation (Metz, 2018). The NFC tag can be applied to both individual evidence and a collection of evidence representing the overall case. By collecting all the hash values and computing a new bundled hash, we will know if there are any evidence missing from the collection when we recompute the bundle hash at a later time, similar to the root hash of the merkle tree previously discussed. With the limited storage an NFC tag can contain, we must decide of what data to be added, but for investigative purposes, individual digital evidence tags must as a minimum requirement contain the evidence hash value. Additional elements may be the information regarding the initial collection and data regarding the case of which the evidence is relating to. An important notice regarding the tags is that even though NFC provide additional security in its limited communication distance, it can still be targeted by several types of known attacks such as man-in-the-middle, eavesdropping, relay attack, and spoofing (Paganini, 2013). Considering that the implementation of this project is meant to be used in a secure area with limited access in addition to the reduced NFC signal distance, it should mitigate the probability of having a potential attacker intercepting the transmission at close range.

5.7 Interview summary

During the course of this project there were several sources of information to be reviewed and analysed. One of the most giving informative sources were the interviews conducted. There was a total of two separate qualitative interviews conducted during this project and both sources provided great insight into their respective fields and professional views of the topic at hand. This chapter summarise a brief overview of the data collected regarding the forensics processes and methods that the two participants were able to provide. To maintain anonymity of the participants, this report will refer to the individuals as digital forensics investigator A and digital forensics investigator B. The table below (table 4) will state the forensics practise and describe the process the individual participants were able to provide regarding a relative process within their respective organisation.

Table 4

	Digital forensics investigator A	**Digital forensics investigator B**
Collection phase	Provided by client or by authorised acquisition	Authorised acquisition
Imaging	Evidence is imaged using forensically sound tools	Evidence is imaged using forensically sound tools
Integrity preservation	Computed hash value	Computed hash value
Chain of custody	Followed and documented throughout the whole evidence life cycle	Followed and documented throughout the whole evidence life cycle
Physical digital media storage	Controlled and secure evidence lockers	Controlled and secure evidence storage
Access to digital evidence	Limited access with an electronic chip at daytime and combined with a passcode after hours	Limited permission-based access to storage using ID card and passcode
Regulations and policy	Best practice based on ACPO principles	Best practise based on documented and proven standards
Thoughts on a blockchain solution	May prove to be useful, but current solutions are sufficient for now as well	Might be a useful solution as long as security and efficiency remain on the same level or higher
Thoughts on tag implementation	Could save time and effort	Could be a useful implementation

CHAPTER 6: INTEGRATION, DESIGN AND IMPLEMENTATION

The solutions and methods discussed in this project consists of functionalities that must be integrated to give the project the many capabilities which are proposed through this report. The purpose of this chapter is to put everything together and integrate the solutions in a setting which may have use for its functionalities when it comes to evidence handling. Considering the context of which the solution is to be implemented, the use of a distributed network is obviously less applicable if it is used by a single workstation or local office. This solution may be more useful for an organisation with several locations which is sharing network and resources. In the sense of applying this project to an organisation and while using a proof of authority (PoA) consensus, the term distributed network is more appropriate rather than calling it decentralised.

6.1 Proposed system solution

The process of evidence handling in relation to this project starts with the first responder and first contact with the evidence. It is at this point in time of which the chain of custody for the evidence must be implemented into the forensics process. The basic rules are to document all actions the investigator takes and take all appropriate steps to ensure that the evidence is not compromised in any way during the acquisition (Schultz & Shumway, 2001, p. 169). The integrity of the digital evidence is heavily dependent on the investigator to make the right decisions. After the evidence have been safely and properly collected, the next step is to create a forensically sound copy of the evidence using trusted imaging tools and create a hash to preserve integrity. As discussed previously with regards to hashing, it could be wise to perform the same algorithm three times at this stage. Firstly, hashing the original evidence before the imaging process to have safe and certain value. Secondly, to hash the imaged copy of the evidence after the process is finished to have true hash value of the copy (some tools does this be default). Third and finally, hashing the original evidence again, to make sure the process of imaging the evidence did not alter any data and to compare it to the copy for confirmation of a complete and successful process. The type of hash used to verify evidence integrity is up to any user to decide, but as mentioned earlier, SHA-256 is the selected algorithm in this project. In a personal interview with a digital investigator, it was stated that a secure and dependent hash algorithm may have the added effect of deterring question during cross-examination from the defence in a court setting as well as the original evidence integrity preservation. When the unbroken security of a implemented hash algorithm is common knowledge, the defence will not put in any time or effort in an attempt to cast doubt in the investigator's processes (Digital forensics investigator B, 2018, personal interview). As evidence image format it is still, as previously discussed, the E01 format which is the suggested approach in this report, although anyone implementing this proposed solution are free to select whichever format they may desire.

The digital signature variation used to verify the person adding evidence data to the blockchain will in this project be the elliptic curve digital signature algorithm (ECDSA), which is highly used in blockchain technology because of its computational performance and relatively short keys (Heide, 2018). To have control over all the people using their digital signature to submit evidence, the organisation which is implementing this technology will need to have a secure database storing the identity of the person, the person's user-ID, and the corresponding person's public key as a digital certificate. The private key of the individual, which is used to sign their actions and documents, is not meant to be shared with the organisation, or anyone, and must be kept securely in their own possession. No other person should be able to sign any documents, files, or actions which are not endorsed or authorised by the owner of the key. The organisation will in this case be the working trusted certificate authority (CA) in which the employees and partners use to create their digital certificate. When a person requires a digital certificate in order to properly and diligently add evidence data to the blockchain, they issue a certificate request to the authorised section of the organisation which handles these requests and manage the database. The request includes the person's public key, employee/ user id, the person' identity, and other required information listed by the CA (Hazlewood, 2011). If the CA approves the information, then the requesting entity will receive their digital certificate and will be allowed to use their private key to sign work related documents and actions. The signature process is a means of verifying the signing entity, and because the organisation has the

corresponding public key stored, the signing entity can be verified by applying the public key to the signed message to open and view its contents. Rules, behaviour, and management regarding digital certificates and key management should be clearly stated by the organisation to avoid misunderstanding, mismanagement, errors, and issues. Key management is usually provided in the context of a specific security policy (Menezes et al., 1996, p. 545).

The system proposed in this project will consist of three main parts. A user interface to perform actions towards the storage and blockchain, the database or file system where the digital evidence copies are stored, and the blockchain which will be the functional chain of custody for the evidence. As suggested by several solutions discussed previously, the evidence will not be included as part of the blockchain because of the large potential file size an item might have (e.g. terabytes of video evidence), and because evidence would be spread to all network nodes. The purpose of the blockchain is to be a chain of custody, logging actions and access towards evidence in the overall system. The interface accessible for users in the network should be protected with a username (user-ID) and password. The database should store an image copy of the evidence, the hash, last transfer of the evidence (the organisation/ entity/ party who took possession), last time accessed, and existing status (e.g. evidence removed = true/false). An approached to implement electronic tags will be discussed lastly.

When a new piece of digital evidence is introduced to the system, a genesis block will be initialised. A genesis block is the first block in its chain and must include all parameters upon creation, except the hash of a previous block. As a rule, the blockchain should not contain personal identifiable information or sensitive case material because of its open view, and with regards to GDPR. The genesis block of the blockchain when working as a chain of custody should include an incremental block-ID (block height), a timestamp, evidence hash value, user-ID, and a digitally signed description of the evidence (safely verifying the entity in possession). The description would normally include information such as the pertaining case reference and the location of acquisition.

Any subsequent actions towards the evidence, such as access or transfer of evidence, will record the data of the event into the blockchain as transactions. These actions will again include a timestamp, evidence hash, user-ID, and a digitally signed description by that entity of what actions were taken. Signed data can be viewed upon request and permission of the organisation's CA, to receive the signer's public key and decrypt the message, allowing others to examine its contents. Transactions on the blockchain require a digital certificate at the organisation's CA to sign the entity's actions taken towards the evidence. Descriptions of actions are signed for two reasons; encrypting case sensitive information from a wide audience (all nodes), and to make sure that the entity who submitted the transaction is the same person as the user-ID suggests. A separate secure database stores the person's corresponding identity, user-ID, and public key (digital certificate) for verification. The reason it is only the description that is digitally signed and not the entire transaction is because the blockchain is supposed to provide transparency. Having the all transaction data hidden behind cryptography would allow for misconduct and errors to go unseen, unless someone decrypted and examined the transaction after every single new addition to the blockchain. A regular anonymous blockchain may provide a high degree of privacy, but transparency makes people more diligent in their work, knowing their actions might be examined at a later date.

Because the blockchain uses a PoA, it is up to the validator nodes to decide when to insert a new block, but this task should be done with regular intervals and only if pending transactions are available. The subsequent block will then include all the pending transactions while storing an incremented block-ID (block height), a timestamp, a collected hash of all the transactions, ID of the validating node(s), and store the hash of the previous node. Like the evidence hash, the blocks and collected hash utilise the SHA-256 algorithm to provide a required level of security for the blockchain.

All access to the evidence is required to be documented into the chain of custody (blockchain) using the interface. The attributes to be added when accessing evidence should be a timestamp, evidence hash, user-ID, and a digitally signed description of actions taken towards the evidence.

Actions such as collecting evidence from the storage needs to include a log entry of the action of collecting it from storage, and a log entry of the return after use. The reason hash is a part of this process is to make sure no alterations took place. Entities outside the network such as prosecutors and other parties must be granted access before they can view the contents of the blockchain and examine the chain of custody.

If evidence is requested to be removed due to overextended retention regulations/ policy or other reasons, it may be removed from the database, any file system, and physical storage without affecting the documentation stored in the blockchain. The signed/ encrypted evidence is still available for examination through request, but if the removal of evidence and case history is highly sensitive and severe, the encryption keys may be erased as well to deny all future examination of the signed data. Removing evidence must be authorised by a senior investigator, case supervisor, or similar entity with the required authority and permissions, and can be accomplished through the interface by stating the entity's user-ID, evidence hash, and a digitally signed description of reason behind erasure. This signature will again prove that the authenticity of the entity.

Evidence transfer can be accomplished through a transaction. This transaction, compared to normal access, will require that the user-ID of both parties are submitted, a timestamp, evidence hash value, and a digitally signed description of any actions involved in the process. This description would preferably be signed by both parties, but might be difficult if evidence is transferred to another organisation which does not implement this system. The suggested approach would then be to print out the full unencrypted chronological history of the chain of custody from the blockchain, and provide it to entity who took possession of the evidence. The information and evidence hash of the last transaction on the printout of the blockchain should be reflected as the first entry of the receiving entity's chain of custody form.

6.2 Electronic tag implementation

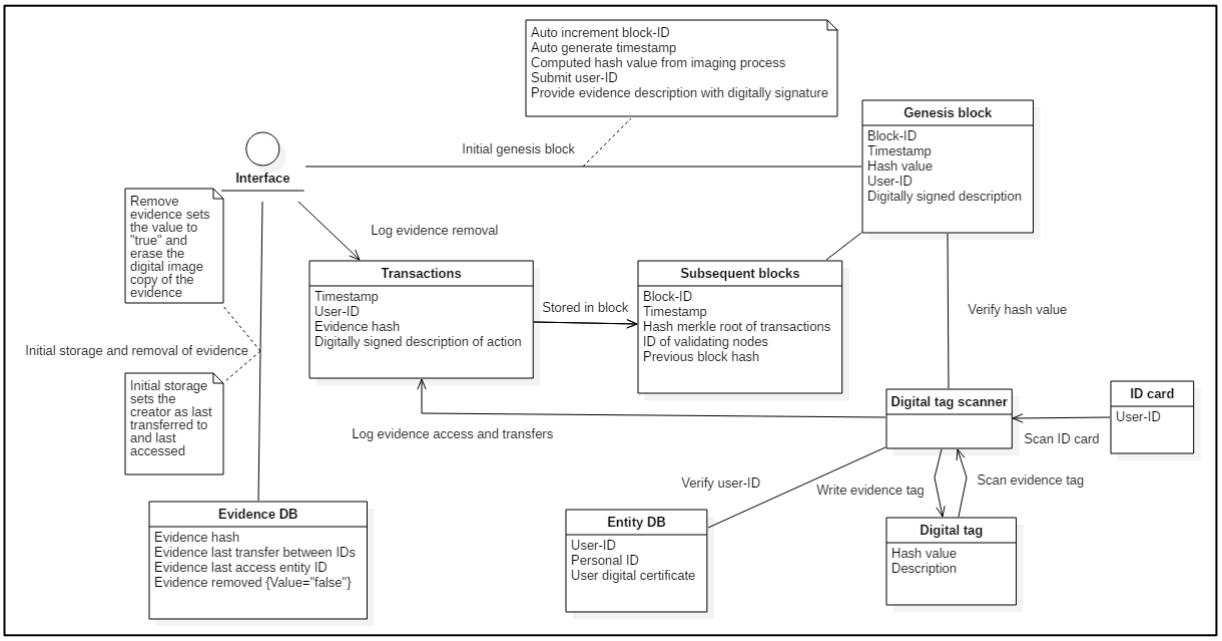
Now that considerations towards the system security and functionality is secure we can move on to the physical aspect of the evidence. Protecting the integrity of the evidence also involves the digital media where the evidence is electronically stored. As previously discussed, digital evidence must be handled with great care because of its fragile nature, and the storage area must be secured against unauthorised access, have lock mechanisms, and a limited distribution of keys. To follow the chain of custody, all actions towards the evidence must be accurately documented for later examination. Evidence must be accounted for the entire time it is in custody. Preserving evidence can be tedious, but lack of attention to details can ruin the case when the evidence turns out to be inadmissible in court (Kruse II & Heiser, 2001, p. 19).

The electronic tag approach is an attempt to semi-automate the chain of custody process by implementing electronic tags to the evidence and integrate it as part of the blockchain system. As mentioned earlier, the technology to be used is the near-field-communication (NFC) and it will store information as a passive tag implementation. As previously stated regarding blockchain transactions, we need to have a timestamp, user-ID, the hash value, and a description of actions when accessing evidence. By having tags store the evidence hash and other relevant information, we can efficiently reduce the work by having this information automatically read of a tag when using a scanner (e.g. wireless handheld, wired handheld, or separate machine located in the storage area). The scanner may then read the required information of the evidence tag (hash and description data such as case reference and acquisition location), and then get the user-ID scanned of a personnel ID card. The hash integrity can be verified by automatic comparison to the original submission into the blockchain, and user-ID can be verified towards the personnel database for an existing valid id. Digital signature with a private key will still be provided by the person handling the evidence, whose key is never disclosed to anyone. The signature prevents any other entity, people or organisations, to authorise or endorse actions on the behalf of the individual. Tag information is only written once before the tag is locked. This is because data stored is never supposed to be changed. NFC tag information must be encrypted to only allow it to be read by the appropriate scanner, as a wide range of smart phones have this technology integrated as well (Unitag, 2018). It would be possible to use a work issued phone as a scanner as well, but it will require additional security concerns and application development.

An evidence locker containing several pieces of evidence could have a tag placed on the locker as well as on each piece of evidence. The locker tag would contain a description of the collection of evidence as well as a hash computed from the sum of all the evidence stored within the collection. A routine based inspection of the evidence would uncover if any pieces of evidence are missing from the locker if the collection of evidence hashes does not equal the hash from the corresponding evidence locker tag.

The figure below is a first edition draft of a proposed implementation design of the discussed system solution (figure 8). It illustrates the integration of the technologies and functionalities suggested and analysed throughout the report.

Figure 8



CHAPTER 7: DISCUSSION AND CONCLUSION

The proposed implementation and design cover and extend the digital integrity preservation aspect of digital forensics. There will always be ways and attempts to trick a system and find weaknesses, but security flaws can hopefully be mitigated by implementing a blockchain solution as the one proposed in this report. For the "integrity before collection" issue, we still cannot ensure integrity before the evidence is collected. The only solution seen so far is the video evidence services discussed previously which computes evidence hash immediately after an event occurred (Gipp et al., 2016; Sugrue, 2018). However, blockchain capabilities such as the transparency of actions and the digital signature implementation may also hinder potential insider attacks from occurring by making it more difficult to accomplish anonymous actions towards the evidence.

After reviewing digital evidence solutions and gaining a view of professional organisational solutions through interviews, it is clear that a blockchain implementation can provide additional security and functionality to current methods. Blockchain technology certainly have the capabilities to protect the integrity of electronically stored evidence with a proper implementation. The added digital tag technology to reduce human error and automated chain of custody received positive feedback from the interviews conducted on the digital forensics investigators working within their respective professional sectors. Although the level of security provided through blockchain might be excessive in most cases, it might be necessary in some sectors where intrusion or danger of insider attacks are greater. Current digital evidence solutions do not support the same level of immutability and transparency that a blockchain based chain of custody could provide for the evidence. The blockchain based solution implemented with a digital tag system would allow for immutability, distribution, transparency, efficient evidence management, and an undisputed control over individual actions that are digitally signed off by the professional entity.

This project is limited to an area with a small audience and few professionals with knowledge within the topic. Research conducted throughout this project might be limited because of this issue and could therefore be affected by the narrow array of people with expertise within the field. Extensions to this project and future work would involve the development of a working prototype and further evaluate its practical functionality and effectiveness.

REFERENCES

Accenture. (2017). *Cost of Cyber Crime Study*. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Bashir, I. (2018). *Mastering Blockchain* (Second). Birmingham: Packt Publishing Ltd.

Boness, D. K. D. (2017). *PROOF-CERTIFICATES as a SERVICE*. Retrieved from https://www.ept.gi/techpaper/Evident-Proof Service Technical Whitepaper v3-0.pdf

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). *B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics*. Retrieved from https://arxiv.org/abs/1807.10359v1

Bonsor, K., & Fenlon, W. (2007). How RFID Works. Retrieved September 29, 2018, from https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid1.htm

Britz, M. T. (2013). *Computer Forensics and Cyber Crime - An Introduction* (Third). Boston: Pearson.

Buchanan, W. J. (2017). *Cryptography*. River Publishers.

Buterin, V. (2015). On Public and Private Blockchains. Retrieved September 24, 2018, from https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Catalyst. (2016). Our Products. Retrieved September 29, 2018, from https://www.catalyst-direct.com/us/

Chandler, N. (2012). What's the difference between RFID and NFC? Retrieved September 29, 2018, from https://electronics.howstuffworks.com/difference-between-rfid-and-nfc.htm

Ćosić, J., & Bača, M. (2010a). (Im)proving chain of custody and digital evidence integrity with time stamp. IEEE. https://doi.org/10.13140/RG.2.1.1336.0725

Ćosić, J., & Bača, M. (2010b). Do We Have Full Control Over Integrity in Digital Evidence Life Cycle? In *The ITI 2010, 32nd International Conference on Information Technology*. Cavtat, Croatia: IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/5546413/?part=1

Curran, B. (2018). What is a Merkle Tree? Beginner's Guide to this Blockchain Component. Retrieved September 21, 2018, from https://blockonomi.com/merkle-tree/

Davidson, A. (2017). Increasing trust in criminal evidence with blockchains. Retrieved July 21, 2017, from https://mojdigital.blog.gov.uk/2017/11/02/increasing-trust-in-criminal-evidence-with-blockchains/

Delfs, H., & Knebl, H. (2002). *Introduction to Cryptography*. Berlin: Springer.

Department of Defence. (2010). DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3), (DoDD 5505.13E). Retrieved from http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/550513E.pdf

Digital forensics investigator B. (2018). *Digital Forensics Interview*.

Doyle, S. (2018). The importance of the audit chain for video evidence. Retrieved September 20, 2018, from https://www.kinesense-vca.com/2018/01/22/the-importance-of-the-audit-chain-for-video-evidence/

Evident-Proof. (2017). *Evident Proof Token Whitepaper* (No. V2.7). Retrieved from https://www.ept.gi/whitepaper/Evident Proof Token Whitepaper - V2.7.pdf

Faulkner, C. (2017). What is NFC? Everything you need to know. Retrieved September 29, 2018, from https://www.techradar.com/news/what-is-nfc

Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. Wiley Publishing Inc.

Floyd, D. (2017). Merkle Tree. Retrieved September 21, 2018, from https://www.investopedia.com/terms/m/merkle-tree.asp

Fowler, E. (2018). Burden of Proof - Evidence for Blockchain's Killer Use Case. Retrieved from https://www.cbronline.com/in-depth/evidence-blockchain-killer-use-case

Garfinkel, S. L., Malan, D. J., Dubec, K.-A., Stevens, C. C., & Pham, C. (2006). ADVANCED FORENSIC FORMAT: AN OPEN, EXTENSIBLE FORMAT FOR DISK IMAGING. In *Second Annual IFIP WG 11.9 International Conference on Digital Forensics. Orlando*. Retrieved from https://cs.harvard.edu/malan/publications/aff.pdf

Gates, M. (2017). *Blockchain: Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money*. Wise Fox Publishing.

Gipp, B., Kosti, J., & Breitinger, C. (2016). Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain. In *MCIS 2016 Proceedings 51*. Retrieved from http://aisel.aisnet.org/mcis2016/51

Gordon, S. A. (2018). What is NFC and why should I use it? Retrieved September 29, 2018, from https://www.androidpit.com/what-is-nfc

Grimes, R. A. (2017). All you need to know about the move from SHA-1 to SHA-2 encryption. Retrieved September 27, 2018, from https://www.csoonline.com/article/2879073/encryption/all-you-need-to-know-about-the-move-from-sha1-to-sha2-encryption.html

Haber, S., & Stornetta, W. S. (1991). *How to Time-Stamp a Digital Document*. Morristown. Retrieved from https://www.anf.es/pdf/Haber_Stornetta.pdf

Hazlewood, L. (2011). What is an X.509 Certificate? Retrieved September 30, 2018, from https://stormpath.com/blog/what-x509-certificate

Heide, D. Ter. (2018). A Closer Look At Ethereum Signatures. Retrieved September 30, 2018, from https://hackernoon.com/a-closer-look-at-ethereum-signatures-5784c14abecc

Hertig, A. (2017). How Ethereum Works. Retrieved September 20, 2018, from https://www.coindesk.com/information/how-ethereum-works/

Hidglobal. (2018). HID® RFID Tags. Retrieved September 29, 2018, from https://www.hidglobal.com/products/rfid-tags

Holcomb, N. (2013). 2D Barcode Symbologies. Retrieved September 29, 2018, from http://www.systemid.com/learn/2d-barcode-symbologies/

Hosmer, C. (2002). Proving the Integrity of Digital Evidence with Time. *International Journal of Digital Evidence*, *1*(1). Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf

International Organization for Standardization. (2012). ISO/IEC 27037:2012. Retrieved September 8, 2018, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

Jayachandran, P. (2017). The difference between public and private blockchain. Retrieved September 24, 2018, from https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Jimi S. (2018a). Blockchain: how a 51% attack works (double spend attack). Retrieved September 25, 2018, from https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474

Jimi S. (2018b). Blockchain: how mining works and transactions are processed in seven steps.

Retrieved September 24, 2018, from https://blog.goodaudience.com/how-a-miner-adds-transactions-to-the-blockchain-in-seven-steps-856053271476

Kenan, K. (2005). *Cryptography in the database*. Upper Saddle River, NJ: Addison-Wesley.

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *National Institute of Standards and Technology*, (Special Publication 800-86). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Khatwani, S. (2018a). What Are Private Blockchains & How Are They Different From Public Blockchains? Retrieved September 24, 2018, from https://coinsutra.com/private-blockchain-public-blockchain/

Khatwani, S. (2018b). What is a Bitcoin Hash? Retrieved September 27, 2018, from https://coinsutra.com/bitcoin-hash/

Khatwani, S. (2018c). What is Double Spending & How Does Bitcoin Handle It? Retrieved September 25, 2018, from https://coinsutra.com/bitcoin-double-spending/

Kruse II, W. G., & Heiser, J. G. (2001). *Computer Forensics: Incident Response Essentials*. Boston: Addison Wesley.

Lehpamer, H. (2012). *RFID Design Principles* (Second). Boston: Artech House.

Liu, C. (2017). How the Blockchain Could Transform the Process of Documenting Electronic Chain of Custody. Retrieved August 6, 2018, from https://venturaerm.com/Blog/10.html

Lone, A. H., & Mir, R. N. (2017). FORENSIC-CHAIN: ETHEREUM BLOCKCHAIN BASED DIGITAL FORENSICS CHAIN OF CUSTODY. *Scientific and Practical Cyber Security Journal*, (2). Retrieved from https://journal.scsa.ge/issues/2017/12/783

Lord, N. (2018). A DEFINITION OF GDPR (GENERAL DATA PROTECTION REGULATION). Retrieved September 26, 2018, from https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

Lowrysolutions. (2015). What Is the Difference Between 1D and 2D Barcode Scanning? Retrieved September 29, 2018, from https://lowrysolutions.com/blog/what-is-the-difference-between-1d-and-2d-barcode-scanning/

Lynch, V. (2017). Re-Hashed: The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms. Retrieved September 27, 2018, from https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/

Menezes, A. J., Oorschot, P. C. van, & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. Boca Raton: CRC Press LLC.

Metz, R. (2018). This company embeds microchips in its employees, and they love it. Retrieved September 29, 2018, from https://www.technologyreview.com/s/611884/this-company-embeds-microchips-in-its-employees-and-they-love-it/

Mitchell, B. (2018). What is a Denial of Service? Retrieved September 21, 2018, from https://www.lifewire.com/denial-of-service-dos-and-ddos-817997

Mougayar, W. (2016). *The Business Blockchain*. John Wiley & Sons, Inc.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.

National Crime Agency. (2016). *Cyber Crime Assessment 2016*. Retrieved from

http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

Naumoff, A. (2017). Why Blockchain Needs 'Proof of Authority' Instead of 'Proof of Stake.' Retrieved September 24, 2018, from https://cointelegraph.com/news/why-blockchain-needs-proof-of-authority-instead-of-proof-of-stake

Nelson, B., Phillips, A., & Steuart, C. (2015). *Guide to Computer Forensics and Investigations: Processing Digital Evidence* (Fifth). Cengage Learning.

Newman, R. C. (2007). *Computer Forensics*. Boca Raton: Auerbach Publications.

Paganini, P. (2013). Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema. Retrieved September 29, 2018, from https://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/#gref

Parker, L. (2016). Private versus Public Blockchains: Is there room for both to prevail? Retrieved September 24, 2018, from https://magnr.com/blog/technology/private-vs-public-blockchains-bitcoin/

POA Network. (2017). Proof of Authority: consensus model with Identity at Stake. Retrieved September 21, 2018, from https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

RFID Basics. (2016). How Much Information Can RFID Card Store? Retrieved September 29, 2018, from http://www.asiarfid.com/rfid-basics/how-much-information-can-rfid-card-store.html

RFID Race Timing Systems. (2017). RFID RACE TIMING SOLUTIONS. Retrieved September 29, 2018, from https://rfidtiming.com/

Rouse, M. (2009). bar code (or barcode). Retrieved September 29, 2018, from https://searcherp.techtarget.com/definition/bar-code-or-barcode

Rouse, M. (2016). asymmetric cryptography (public key cryptography). Retrieved September 28, 2018, from https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

Rouse, M. (2018). digital certificate. Retrieved September 28, 2018, from https://searchsecurity.techtarget.com/definition/digital-certificate

Rykwalder, E. (2014). The Math Behind Bitcoin. Retrieved September 28, 2018, from https://www.coindesk.com/math-behind-bitcoin/

Salgado, D. (2016). *Blockchain of Evidence*. Retrieved from https://docs.google.com/document/d/1rGHNzrZsMSIDQgFSXVNrRuBYXdPlhfUFWZM3JGmjvv0/edit#

Schofield, J. (2015). What is a Barcode Scaner and How Does it Work? Retrieved September 29, 2018, from http://www.systemid.com/learn/barcode-scanners-and-how-they-work/

Schultz, D. E. E., & Shumway, R. (2001). *Incident Response: A Strategic Guide to Handling System and Network Security Breaches* (First). Boston: New Riders Publishing.

Shilov, K. (2018). When is it Time to Build Your Own Blockchain? Retrieved September 24, 2018, from https://hackernoon.com/when-is-it-time-to-build-your-own-blockchain-f3be0a30b826

Shinder, D. L., & Tittel, E. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress Publishing, Inc.

ShopNFC. (2018). NFC Tags Specs. Retrieved September 29, 2018, from https://www.shopnfc.com/en/content/6-nfc-tags-specs

Solomon, M. G., Rudolph, K., Tittel, E., Broom, N., & Barrett, D. (2011). *Computer Forensics JumpStart* (2nd ed.). Wiley Publishing, Inc.

Stone, A. (2015, September). Chain of Custody: How to Ensure Digital Evidence Stands Up In Court. *Govtech Works*. Retrieved from https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/

Sugrue, M. (2018). Blockchain and Digital Chain of Evidence. Retrieved July 23, 2018, from https://www.kinesense-vca.com/2018/03/13/blockchain-and-digital-chain-of-evidence/

SWGDE. (2017). *SWGDE Best Practices for Maintaining the Integrity of Imagery*. Retrieved from https://www.swgde.org/documents/Current Documents/SWGDE Best Practices for Maintaining the Integrity of Imagery

SWGDE Best Practices for Computer Forensics. (2014). SWGDE Best Practices for Computer Forensics, (Version 3.1). Retrieved from https://www.swgde.org/documents/Current Documents/SWGDE Best Practices for Computer Forensics

SWGIT. (2010). *Best Practices for Maintaining the Integrity of Digital Images and Digital Video*. Retrieved from https://www.swgit.org/pdf/Section 13 Best Practices for Maintaining the Integrity of Digital Images and Digital Video?docID=54

SWGIT. (2015). Scientific Working Group on Imaging Technology. Retrieved September 14, 2018, from https://www.swgit.org/

Tar, A. (2018). Proof-of-Work, Explained. Retrieved September 21, 2018, from https://cointelegraph.com/explained/proof-of-work-explained

The European Parlament and the Council of the European Union. (2016). Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Thrasher, J. (2013). How is RFID Used in Real World Applications? Retrieved September 29, 2018, from https://blog.atlasrfidstore.com/what-is-rfid-used-for-in-applications

Triggs, R. (2018). What is NFC & how does it work? Retrieved September 29, 2018, from https://www.androidauthority.com/what-is-nfc-270730/

Unitag. (2018). NFC compatible phone list. Retrieved October 2, 2018, from https://www.unitag.io/nfc/is-my-phone-compatible-with-nfc

Vandeven, S. (2014). *Forensic Images: For Your Viewing Pleasure*. Retrieved from https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447

Volonino, L., Anzaldua, R., Godwin, J., & Kessler, G. C. (2006). *Computer Forensics Principles and Practices*. Pearson Prentice Hall.

Williams, J. (2012). *ACPO Good practice Guide for Digital Evidence. Metropolitan Police Service, Association of chief police officers, GB* (Vol. 1). Retrieved from http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

Windley, P. J. (2005). *Digital Identity* (First). Beijing: O'Reilly Media, Inc.

Zenner, E. (2009). *Nonce Generators and the Nonce Reset Problem* ((eds) Information Security No. Samarati P., Yung M., Martinelli F., Ardagna C.A). *ISC 2009*. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-04474-8_33

Figures and tables

Figure 1:
Accenture. (2017). *Cost of Cyber Crime Study*. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-1/Accenture-2017-CostCyberCrimeStudy.pdf

Figure 2:
Salgado, D. (2016). *Blockchain of Evidence*. Retrieved from https://docs.google.com/document/d/1rGHNzrZsMSIDQgFSXVNrRuBYXdPlhfUFWZM3JGmjvv0/edit#

Figure 3:
Gipp, B., Kosti, J., & Breitinger, C. (2016). Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain. In *MCIS 2016 Proceedings 51*. Retrieved from http://aisel.aisnet.org/mcis2016/51

Figure 4:
Sugrue, M. (2018). Blockchain and Digital Chain of Evidence. Retrieved July 23, 2018, from https://www.kinesense-vca.com/2018/03/13/blockchain-and-digital-chain-of-evidence/

Figure 5:
Lone, A. H., & Mir, R. N. (2017). FORENSIC-CHAIN: ETHEREUM BLOCKCHAIN BASED DIGITAL FORENSICS CHAIN OF CUSTODY. *Scientific and Practical Cyber Security Journal*, (2). Retrieved from https://journal.scsa.ge/issues/2017/12/783

Figure 6:
Floyd, D. (2017). Merkle Tree. Retrieved September 21, 2018, from https://www.investopedia.com/terms/m/merkle-tree.asp

Figure 7:
Bonomi, S., Casini, M., & Ciccotelli, C. (2018). *B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics*. Retrieved from https://arxiv.org/abs/1807.10359v1

Table 1:
Hosmer, C. (2002). Proving the Integrity of Digital Evidence with Time. *International Journal of Digital Evidence*, *1*(1). Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf

Table 2:
Ćosić, J., & Bača, M. (2010a). (Im)proving chain of custody and digital evidence integrity with time stamp. IEEE. https://doi.org/10.13140/RG.2.1.1336.0725

Table 3:
SWGDE. (2017). *SWGDE Best Practices for Maintaining the Integrity of Imagery*. Retrieved from https://www.swgde.org/documents/Current Documents/SWGDE Best Practices for Maintaining the Integrity of Imagery