Blockchain-based Chain of Custody

Towards Real-time Tamper-proof Evidence Management

Liza Ahmad[†]
College of Technological Innovation
Zayed University
Abu Dhabi UAE
liza.ahmad@zu.ac.ae

Salam Khanji
College of Technological Innovation
Zayed University
Abu Dhabi UAE
M80006416@zu.ac.ae

Farkhund Iqbal
College of Technological Innovation
Zayed University
Abu Dhabi UAE
Farkhund.iqbal@zu.ac.ae

Faouzi Kamoun
ESPRIT School of Engineering
Tunis Tunisia
faouzi.kammoun@esprit.tn

ABSTRACT

Evidence is a tangible demonstrative artifact that proves a fact and shapes the investigation of various misconduct cases involving for instance corruption, misbehavior, or violation. It is imperative to maintain proper evidence management to guarantee the admissibility of an evidence in a court of law. Chain of custody forms the forensic link of evidence sequence of control, transfer, and analysis to preserve evidence's integrity and to prevent its contamination. Blockchain, a distributed tamper-resistant ledger can be leveraged to offer a decentralized secure digital evidence system. In this paper, we propose a secure chain of custody framework by utilizing the blockchain technology to store evidence metadata while the evidence is stored in a reliable storage medium. The framework is built on top of a private Ethereum blockchain to document every transmission from the moment the evidence is seized, thus ensuring that evidence can only be accessed or possessed by authorized parties. The framework is integrated with the digital evidence system where evidence is physically stored and locked using smart locks. To secure the sequence of evidence submission and retrieval, only an authorized party can possess the key to unlock the evidence. Our proposed framework offers a secure solution that maintains evidence integrity and admissibility among multiple stakeholders such as law enforcement agencies, lawyers, and forensic professionals. The research findings shed light on hidden opportunities for the efficient usage of blockchain in other realms beyond finance and cryptocurrencies.

ARES 2020, August 25–28, 2020, Virtual Event, Ireland

ACM ISBN 978-1-4503-8833-7/20/08…$15.00
https://doi.org/10.1145/3407023.3409199

CCS CONCEPTS

• **Computer systems organization → Applied computing**; Computer forensics; • **Security and Privacy** → Systems security; Network security.

KEYWORDS

Digital forensics, Chain of custody, Blockchain, Distributed ledger, Security and privacy.

ACM Reference format:

Liza Ahmad, Salam Khanji, Farkhund Iqbal, and Faouzi Kamoun 2020. Blockchain-based Chain of Custody Towards Real-time Tamper-proof Evidence Management. In *Proceedings of ACM ARES 2020 conference (ARES' 20). ACM, August, 2020, Dublin, Ireland 8 pages.* https://doi.org/10.1145/3407023.3409199

1 Introduction

The main requirements of Internet users are publishing and acquiring content over digital media such as webpages, audios, and videos. Digital contents are vulnerable to network attacks where vicious code can be injected to illegally access private information. Consequently, it is essential to maintain three basic security properties of any digital content: integrity, trustworthiness, and non-repudiation so as to guarantee the admissibility of the corresponding digital evidence in a court of law. When digital evidence is acquired, it is communicated directly to a third-party management to be stored in a local storage (digital evidence system) and to be accessed by any authorized party involved in the forensic process, such as law enforcement and forensic professionals. Most of the existing digital evidence systems utilize a centralized architecture through tamper-resistant mechanisms such as secure hardware and software, or hybrid techniques [1][2]. However, these systems are prone to security risks, single point of failure, and scalability issues that are often associated with large-scale centralized file/storage systems.

Chain of custody is the chronological documentation that records the sequence of control, transfer, analysis, and disposition of evidence in a digital evidence system [3]. As with any digital system, the digital evidence system is vulnerable to data tempering where the evidence can be modified or altered, and it is also susceptible to privacy leaks where private information can be exposed and misused. Chain of custody is a key element in digital forensics where it provides a log file to record and trace all actions related to evidence retrieval, analysis, and alteration from the moment it is collected by the first responder. A record of the chain of evidence must be maintained and established in the court whenever there is a need to present the corresponding evidence as an exhibit[4], otherwise, the evidence might be rejected in the court, leading to serious concerns regarding its integrity, legitimacy, and all analysis rendered upon it [4]. Thus, chain of custody process must be flexible and efficient to facilitate the digital investigation process while ensuring a secure and tamper-proof evidence management. In this contribution, we propose to leverage the blockchain technology to tackle these challenges by taking advantage of its decentralized, distributed, and tamper-resistant features in order to provide the digital transformation of provenance information related to chain of custody process and hence a more secure digital evidence system.

In this research paper we propose a secure blockchain-based chain of custody framework where a private lightweight blockchain is built on top of Ethereum to allow authenticated participants to access off-chain evidence that is stored on a reliable storage medium and locked using smart locks. The framework records all actions conducted on each collected evidence on the blockchain, starting from the first responder who acquired the evidence and all subsequent analysis and modifications so as to ensure evidence admissibility and tamper-proof management when presented in prosecutions. The remainder of the paper is organized as follows: Section 2 presents a literature review on previous work related to blockchain integration into evidence management and chain of custody. Section 3 describes the proposed framework, its design specifications and its security requirements. This section also presents some performance evaluation results to demonstrate the capability of the proposed framework in meeting security and privacy needs in forensic chain of custody. Finally, Section 4 presents concluding remarks and suggestions for future research.

2 Related Work

The increasing dependence on digital technologies has triggered a high demand for the analysis of digital data for the purpose of forensics and digital investigations. In fact, the rapid adoption and diffusion of digital technologies has led to a rise in cybercrimes, which requires the use of digital forensics systems to collect, process, analyze, and report evidence while, at the same time, guarantying the integrity of the evidence and its admissibility in the court of law. The success of blockchain technology in preventing tampering of public ledgers has stimulated its application in new areas that require anti-tampering measures to preserve evidence. [5] presents a prototype blockchain- based Chain of Custody (B-CoC) for digital evidence that is based on Ethereum. B-CoC uses private and permissioned blockchain to ensure that only authorized access is permitted. The B-CoC presented in [5] consists of 3 components: Evidence database (Database with digital evidence), evidence log (CoC related data and hash of evidence), and frontend interface (interface between B-CoC and users). The evidence log is implemented using blockchain and contains information such as evidence ID, evidence description, creator's identity, and owners' history. The evidence log is implemented on a peer-to-peer network that consists of validator entities (such as main coordinator of the court) and lightweight entities (such as forensic investigator). The process of implementing the evidence log consists of three phases. First, the private blockchain is initialized, then the private network is created, and finally, Smart contracts are created and deployed on top of the blockchain infrastructure. Other systems which use a loose-coupling structure to maintain the evidence and the evidence information independently are presented in [6],[7], and [8]. In [6] authors present Block-DEF, a blockchain-based secure and scalable digital evidence framework. The approach stores the evidence on a safe platform while storing the evidence information in the blockchain. This framework uses a lightweight blockchain that combines an optimized name-based byzantine fault-tolerant consensus mechanism with a mixed block structure. Block-DEF consists of three layers: a service layer, a blockchain layer, and a network layer. The service layer consists of evidence-related services, the blockchain layer consists of blockchain and consensus mechanisms, while the network layer is based on Peer-to-Peer networking. Block-DEF adopts a multi-signature scheme using random keys and certificated key pairs to ensure privacy and traceability. Moreover, [10] demonstrates a blockchain-based digital forensics chain of custody using Hyperledger Composer, named Forensic-chain. In Forensic-chain, evidence is kept in a distributed storage that only authorized participants (e.g., prosecutors) can access. Forensic-chain uses a blockchain peer-to-peer network and a consensus protocol to regulate it. Lastly, [8] presents a framework that enables a fact-based confidence rating of digital evidence. In [8] digital evidence is stored in a blockchain that stores the information related to the evidence and is accessible to all authorized involved parties. An external data structure named Forensics Confidence Rating is used to enable involved parties measure the certainty and relevance of the digital evidence. Another data structure presented is the Global Digital Timeline which is used to store the chain of events related to the digital evidence.

The above-mentioned frameworks have focused mainly on ensuring traceability and non-repudiation of the evidence. Our approach, on the other hand, aims to ensure confidentially and trustworthiness of the evidence, in addition to ensuring traceability and non-repudiation. The proposed framework maintains physical evidence and evidence information separately as done in [5],[6],[7], and [8]. However, it also introduces the usage of smart locks in addition to smart contracts to authenticate authorized parties to access the stored physical evidence. Smart

locks are created when a smart contract is created, in order to authenticate and authorize a party that is requesting access to the digital evidence. Smart locks are light Ethereum nodes on the blockchain network where virtual keys are created and destroyed as needed.

Calculating the hash value of digital evidence content and documenting it along with the acquired data may not prove that the digital evidence is the same as when it was seized. In [17] authors present a chronological independently verifiable electronic chain of custody (e-CoC). They propose to utilize a private ledger to maintain chain of custody records excluding sensitive information to guarantee its privacy along with recoding the private ledger status on a public ledger to ensure integrity by its decentralized structure. The use of public blockchain can work to guarantee that the trusted entity responsible for managing the private e-CoC would not intentionally or accidentally modify blocks on e-CoC as they proposed in their simultaneous work in [18]. Our proposed framework deploy a private blockchain hosted by a trusted entity in the same manner as in [17], however, smart locks are used to properly ensure authenticated and authorized access is granted for a requesting party. Consequently, our framework emphasizes on a chronological and timestamped records of chain of custody to maintain a verifiable digital evidence system.

Blockchain technology and forensics can work hand in hand to identity crime or any violations that occur by analyzing useful evidence acquired from different sources. In [9] authors present a new forensic architecture that is integrated in Software Defined Network incorporated with IoT environment. This dual plane (Control/Data) architecture was evaluated using a Network Simulator. Each IoT device sends packets to the gateway which is forwarded to switches. When packets reach the control plane, they are classified after the device signatures have been authenticated. The SDN-controller verifies the signature of data packets using blockchain then classifies packets. These packets get stored as data logs that include user identity, Source IP address, Destination IP address, local time of evidence occurrence, location, and action. An authorized forensics investigator can later access the evidence in the SDN controllers. To maintain trust and integrity of evidence, the hashes of the evidence are stored in the SDN-controller and in the blockchain to maintain the reliability level of the Chain of Custody (CoC). In [10], the authors proposed a private blockchain-based IoT forensics framework that records all events related to the digital evidence during its life cycle. The framework consists of a digital witness, namely a device capable of identifying and collecting digital evidence, and then safely preserving it and sharing it with authorized digital witnesses or digital custodians. The framework in [10] also contains a digital custodian that is represented by a law enforcement entity in charge of collecting evidence. The last entity in this framework is a law enforcement agency that consists of a blockchain platform to record all events related to the evidence, and an evidence analysis platform to analyze all submitted evidences. All entities in the presented framework use public key cryptography for identification. A digital witness, whose identity is bound to its owner, would sign a digital evidence and forward it to digital custodian. This transaction is recorded in the blockchain. A consensus algorithm is used to protect the system from sabotages. Another work related to IoT forensics is [11] where authors introduced Probe-IoT, a framework that uses a public ledger to store evidence emanating from IoT devices. The interactions in the system are stored in public blockchain after being signed by the involved participants and encrypted using a trusted third-party public key. Probe-IoT can be used to investigate cases involving violations of Service level Agreements (SLAs) by service providers.

Among the key challenges associated with the handling of digital evidence in a cloud environment is the potential scattering of the data across various jurisdictional areas. This requires coordination among different parties and the documentation of the resulting chain of custody. In [12], the authors presented a process provenance scheme that guarantees proof of existence and anti-tampering. The scheme aims to meet necessary requirements when several participants are involved, hence increasing the trustworthiness of the chain of custody for cloud forensics. Participants in the scheme consist of (1) the receiver who is usually an investigator submitting a request to the sender to collect forensic data from cloud, and (2) the sender who could be a cloud service provider or another investigator who'd respond with the requested data. The Provenance Auditor receives the process records from all involved parties and anchors the data to a blockchain using the *Chainpoint* proof and anchoring standard. This standard makes it possible to audit the process records to prevent tampering, while providing blockchain receipts. The process records also include the group signatures of the sender and the receiver which are provided by a Certificate Authority. Process records are signed by a group signature which prevents the possibility of tracing the process records back to the sender or the receiver which ensures anonymity. Moreover, to preserve privacy, the process records include only the hash value of the forensics data files submitted by the involved parties.

3 Blockchain-based Chain of Custody Framework

In this section, we first identify the requirements that blockchain-based chain of custody framework must satisfy, and then we introduce the architecture of the proposed framework.

3.1 Framework Requirements

The framework should support evidence collection, storage, verification, possession, and access. The process of blockchain-based chain of custody is composed of three functions: (1) *evidence collection* from the first responder who initiated the process of submitting evidence by creating a new block on the blockchain with a unique address (encrypted pair of private and

public keys), (2) *evidence documentation* that records the required information for the chain of custody such as name of sample collector, contact information, and name of the recipient in the corresponding block in the blockchain that is signed by the party involved in the chain of possession with date and time and (3) *evidence storage* that ties the corresponding evidence address with a smart lock virtual key in a storage medium to ensure authorized evidence access. The proposed framework should fulfill the following requirements:

1. Data Integrity: To guarantee evidence integrity by detecting any modification or alteration that would tamper its truthfulness.
2. Data Trustworthiness and Confidentiality: To ensure that evidence metadata cannot be accessed by unauthorized parties.
3. Data Traceability: To certify the continuity of possession of evidence and its migration from the point of collection and recovery, to its transfer to the forensic labs for analysis and investigation, and until the time it is exhibited in a court of law.

3.2 Framework Architecture

Maintaining the chain of custody is a crucial task in forensic investigation as it logs every action of the examination and analysis of the evidentiary sample to hold liability with any encountering party. This task prevents the involved labs or law officials from tampering the evidence as it would be traceable back to them. However, a trusted storage medium is also vital to securely keep the evidence and to verify its integrity. Our proposed framework provides a secure network channel that can simultaneously tackle security challenges associated with evidence storage media, as well as the chain of custody process. Figure 1 demonstrates the architecture of the proposed framework which consists of three logical layers: (1) evidence layer which supports the trusted storage medium of the evidence through embedding blockchain-based smart locks with private key infrastructure (PKI), (2) blockchain layer which is a private fork built on top of the Ethereum blockchain and controlled by authority organizations due to the sensitivity of the evidence metadata in the forensic examination, and (3) network layer which provides a peer-to-peer communication among the parties in contact with the evidence (including the first responders who seized the evidence, the forensic professionals, and the law enforcement officers).

3.3 Framework Design and Specifications

3.3.1 Evidence Layer: Blockchain-based Smart Locks

This layer presents a smart lock solution to be embedded into the evidence storage medium where it integrates IoT devices and blockchain smart contracts with a flexible web-based interface to allow authenticated parties involved in the forensic process to access evidence data while maintaining its security, integrity, and authenticity. As depicted in Figure 2, when each party in contact with an evidence sample tries to open its lock, the system checks the party permissions and privileges through a smart contract that requests the party unique identifier (assigned from a central authority such as forensic lab) and the designated privileges such as request evidence, examine evidence, or transfer evidence. To address potential computational power requirements and overcome network bandwidth constraints associated with this key step, we used Infura's development suite [13] which provides instant, scalable API to communicate with the private Ethereum fork. Consequently, the solution is very efficient as it simply needs to handle HTTP requests rather than running a full Ethereum node. A forensic party can interact with the blockchain layer through *web3.js* [14], a library used in the web-based interface to open/close evidence smart lock and to record a new sequence in the chain of custody.

When the evidence is first collected and seized by the first responder, he/she broadcasts a transaction through the web-based interface on the blockchain. This process triggers a smart contract to authenticate the first responder and to be validated by authority organizations through proof-of-validity consensus mechanism based on RAFT consensus algorithm [15] that will be explained in more details in Section 3.3.2. Once the transaction is validated, a new smart lock is created that is composed of: hash (first responder IP address) + hash value (evidence name) + hash value (evidence content) using Keccak-256. Moreover, a smart contract is triggered to trace the state of the new smart lock where an issued parameter *i* is set to 1 to indicate that the key is being used. This virtual smart lock key is used to ensure that the smart lock can only change state (open/close) when the request is triggered by the first responder whose IP address matches the IP address in the smart lock itself. Each time a new party needs to access the same evidence for instance, a new virtual smart lock key will be issued. Upon locking the evidence smart lock, the smart contract is triggered again to update the state of the smart lock by setting the parameter *i* to 0, indicating that the key is being handed over and shall be destroyed. This process would ensure evidence integrity and any evidence tampering will be traced back to the IP address of the responder, hence ensuring non-repudiation.

Once the evidence is seized and stored in the trusted storage medium, a specific smart contract is also initiated to log all required information for the chain of custody process. The smart contract logs a unique evidence address where it is designated as a unique evidence identifier (hash (evidence name) + hash (evidence content)), as mentioned earlier. Additionally, it logs laboratory's address, date and time of delivery (the same as timestamp used in the blockchain automatically), and it is signed by keys of both authorized selected leader (according to RAFT consensus mechanism) and the key of the party in contact with the evidence at that particular instance.

3.3.2 Blockchain Layer: Private Ethereum Fork

A private Ethereum fork is created over Google Cloud Compute Engine (Infrastructure-as-a-Service IaaS) to offer a hybrid blockchain solution that enables authorized organization to retain control over the data while cutting down capital expenses and increasing the speed of transactions. Although a private blockchain model does not offer a pure decentralized mechanism

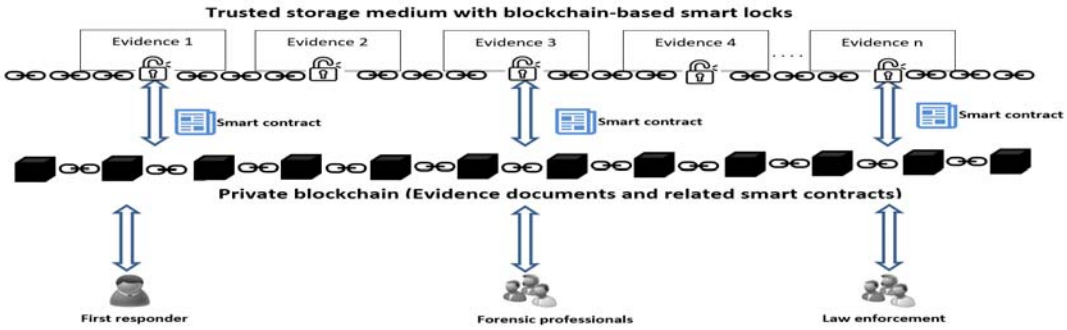

Figure 1: Blockchain-based Chain of Custody Framework

as is the case of its public counterpart model, the model can still inherit valuable blockchain's characteristics such as traceability, integrity, confidentiality, non-repudiation, and it enables the usage of a distributed ledger among all involved parties to keep their files synchronized.

Each block in the blockchain is composed of block header, evidence header, and the body header. The evidence header consists of the evidence unique address, current state of its smart lock, and the sequence of its chain of custody. Each node in the network needs to store the hash of the previous block header, the timestamp, and the Merkel Root that represents the hash value of all transactions in a specific block. When a transaction is broadcasted, it will be verified by a proof-of-validity consensus mechanism, based on the RAFT algorithm. It first elects a distinguished node as a leader which validates the new transaction and leads the whole network to update the distributed blockchain ledger [15], while other nodes act as either followers or candidate nodes. When a leader is disconnected from the network, a new leader is reelected from any candidate nodes while follower nodes remain passive, i.e. and they issue no requests on their own but merely respond to requests from leaders and candidates.

Nodes in the blockchain network communicate using the Remote Procedure Calls (RPCs) protocol where RequestVote RPCs are initiated by candidate nodes during the election process, and AppendEntries RPCs are initiated by leader nodes to update the distributed ledger. Usually, nodes retry RPCs when they do not receive an answer within an elapsed time period, and they also send RPCs to enhance the network performance. The RAFT algorithm utilizes a heartbeat mechanism to elect leader nodes whereby a follower node remains follower if it receives valid RPCs from a leader or a candidate node. The leader node sends AppendEntries RPCs periodically to maintain its authority as a leader. If, for any reason, a follower node does not receive RPCs for a specific time period, it would be assumed that the current leader is no longer valid, and a leader reelection process must be initiated. In the election process, a follower node self-elects itself as a candidate node and sends RequestVote RPCs to all other nodes. All other candidate nodes start voting and the candidate with the majority of votes becomes the leader who will subsequently send a heartbeat message to all other nodes to establish its authority and to stop the election process.

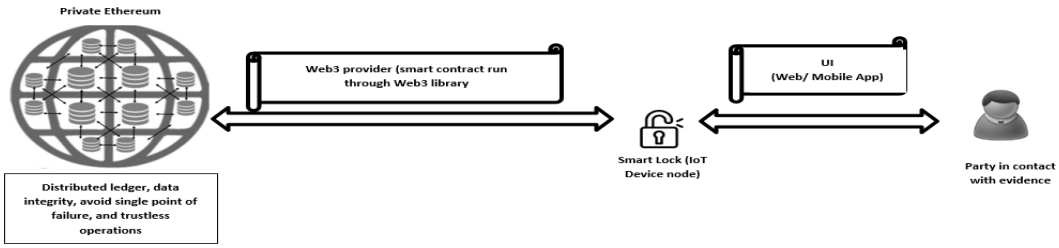

Figure 2: Blockchain-based Smart Lock (Evidence layer in the proposed framework)

3.4 Framework Evaluation

In Section 3.1 we discussed three basic requirements that our proposed framework needs to fulfill: evidence integrity, trustworthiness, and traceability. To validate these requirements, we designed a case scenario to simulate the proposed framework and then assess its ability to meet these three requisites.

3.4.1 Development Environment Figure 3 represents the proposed framework where it consists of two development structures: (1) a centralized web-based interface that resides on Google Cloud App Engine (PaaS: Platform-as-a-Service) to be used by parties in contact with an evidence either as a first responder, forensic professional, or any law enforcement member, and (2) a private fork of Ethereum created on top of Google Cloud Compute Engine (IaaS: Infrastructure-as-a-Service). Simulating the authority organizations requires manual network configuration to create Ethereum nodes (Geth clients) that will control the process of evidence validation through RAFT consensus mechanism. At the same time, smart locks are implemented as light Ethereum nodes on the blockchain network where virtual keys are created/destroyed upon triggering a smart contract to allow or revoke access after validating the ID of any party in contact with evidence. The web-based interface connects with the light Ethereum client running on Raspberry pi (smart lock) via Web3 provider which can be a Web socket provider or HTTP.

3.4.2 Requirements Analysis The proposed framework ensures evidence integrity which can be validated by comparing the hash of its name and the hash of its content. Meanwhile, each time an access to evidence is granted, a new virtual key is created that integrates the hash of requester's IP address and hence all events related to the evidence are committed into the blockchain and can be traced back to the same IP address upon evidence validation. Evidence trustworthiness is also maintained through the extra protection layer imposed by the smart locks that are integrated into the trusted evidence storage off-chain. Consequently, the blockchain is only used to store evidence metadata and not the evidence contents. This design intent aimed at overcoming scalability issues related to blockchains and block sizes.

Moreover, we tested the security level of our proposed framework through analyzing the avalanche effect of both Keccak-256 hashing function and Elliptic Curve Digital Signature Algorithm (ECDSA) encryption mechanism utilized in the private Ethereum fork we developed. The avalanche effect refers to an enviable property of an encryption algorithm where any slight change in the plaintext or the cipher key, the produced output will be significantly changed [16]. Figures 4 and 5 demonstrate the avalanche effect of both Keccak-256 and ECDSA respectively where it depicts that Keccak-256 hash function has an average avalanche effect of 96.8%, hence, Keccak-256 generates a significant output difference with a slight change in input. Additionally, ECDSA encryption has an average avalanche effect of 96.4% as it generates a significant output change with slight changes in input.

Additionally, the RAFT algorithm is utilized to perform the consensus on evidence validation on the private Ethereum blockchain where it places restrictions on who can participate in the network and what privileges to be granted each participant. Consequently, evidence privacy is maintained so that only authorized access is allowed, which can also be traced back for any evidence of potential tampering. Using private blockchain would reduce the computational processing required during the mining process as only a selected node (leader) from a group of authorized organizational nodes will be responsible for confirming transactions and updating the distributed ledger among all network participants. To evaluate the consensus mechanism, we measured the number of network messages in the cases of RAFT consensus mechanism and Istanbul Byzantine Fault Tolerance (IBFT) mechanism in different implementations of permissioned or private blockchain networks. Two network topologies are considered where the number of nodes is set to 1 and 50 nodes as depicted in Figure 6. As may be seen, RAFT resulted in a lower message number compared to IBFT as in the process of updating the distributed ledger, the per AppendEntries RPCs are initiated by the leader node only.

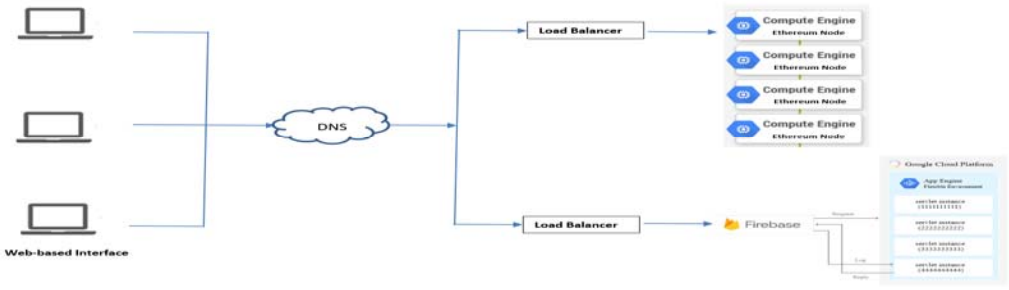

Figure 3: Proposed Framework – Case Scenario

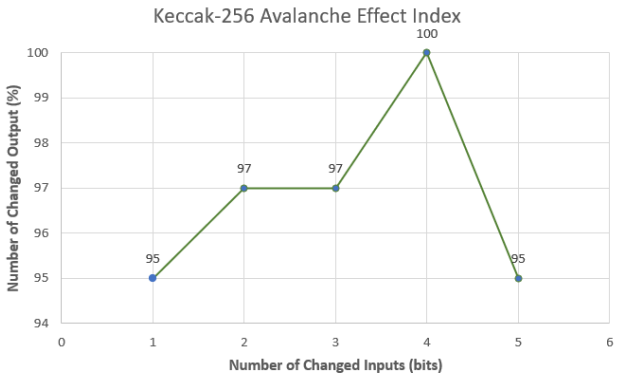

Figure 4: Keccak-256 Avalanche Effect Result

The main difference between IBFT and RAFT algorithms, is that while RAFT followers blindly trust their leader, in IBFT, each block requires multiple rounds of voting by the set of validators to reach a consensus that is recorded as a collection of signatures on the block content. A validator never assumes that the leader is honest. Instead, it verifies the proposed block just like any other consensus platform being deployed on top of an untrusted environment such as Proof-of-Work. Consequently, RAFT consensus does not commit blocks unless there are pending transactions resulting in significant storage efficiency as no empty blocks containing zero transactions are being committed on the blockchain. Moreover, RAFT has a faster block time when compared to IBFT whereby the leader validates a block within 50ms upon receiving the transaction. With RAFT, the election majority acknowledgement is a very fast process as well, as in typical network conditions the average block times are typically in the sub-second range.

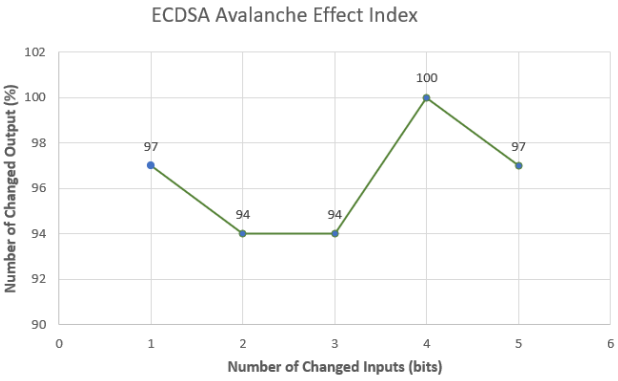

Figure 5: ECDSA Avalanche Effect Result

Our proposed framework can bring substantial benefits to forensic applications by maintaining transparency, integrity, security, and auditability of digital evidence. For instance, it facilitates the process of evidence collection, preserving, and validating the evidence through recording the procedure of its acquisition on the blockchain to allow provenance of any event or action taken on the evidence to be traced back and audited. Moreover, the framework can reduce evidence fraud through increasing transparency where it can be utilized as an auditing tool to support the correctness of the forensic procedures. The proposed framework forms a preliminary foundation of a cross-border forensic investigation to enable broader jurisdictional areas.

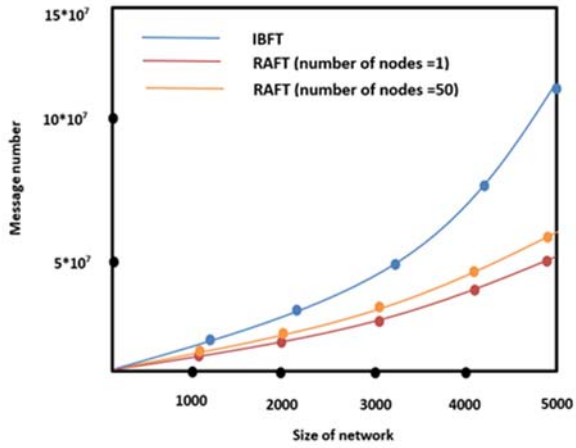

Figure 6: Comparison between Message Numbers of RAFT and IBFT

4 Conclusion

The main aim of this research was to introduce the efficient integration of blockchain technology into digital forensics. For this purpose, we have proposed a digital chain of custody framework that ensures confidentiality, integrity, traceability, and non-repudiation. The three logical layers in the framework implement three key functionalities: (1) the storage of evidence using blockchain-based smart locks, (2) the storage of evidence metadata on top of a private blockchain controlled by a trusted authority, and (3) the communication among involved parties using a peer-to-peer network. The framework is implemented using Ethereum nodes and its performance has been evaluated. The preliminary evaluation results have shown that the proposed framework is able to maintain realistic workloads with an acceptable transaction throughput when compared to other consensus algorithm implementations. The utilization of blockchain ensures evidence content integrity and its admissibility in a court of law by recording the chain of custody on an immutable network. As a future work, we plan to carry additional performance evaluation experiments and further explore the usage of blockchain technology in digital forensics in the quest for new tamper-proof and immutable mechanisms for evidence acquisition and artifact analysis.

REFERENCES

[1] E. Al-Masri, Y. Bai, & J. Li (2018, September). A fog-based digital forensics investigation framework for IoT systems. In 2018 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 196-201). IEEE.

[2] A. Nieto, R. Roman and J. Lopez, (November-December 2016) "Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices," in IEEE Network, vol. 30, no. 6, pp. 34-41.

[3] D. Y. Kao, Y. T. Chao, F. Tsai, & C. Y. Huang (2018, November). Digital Evidence Analytics Applied in Cybercrime Investigations. In 2018 IEEE Conference on Application, Information and Network Security (AINS) (pp. 111-116). IEEE.

[4] H. Paluš, , J. Parobek, R. P. Vlosky, D. Motik, L. Oblak, M. Jošš, ... & L. Wanat (2018). The status of chain-of-custody certification in the countries of Central and South Europe. European journal of wood and wood products, 76(2), pp.699-710.

[5] S. Bonomi & M. Casini & C. Ciccotelli. (2018). B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics.

[6] Z. Tian, M. Li, M. Qiu, Y. Sun, & S. Su. (2019). Block-DEF: A secure digital evidence framework using blockchain. Information Sciences, 491, 151–165. doi: 10.1016/j.ins.2019.04.011

[7] A. Lone, and R. Mir. 2019. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, pp.44-55.

[8] D. Billard. (2018). Weighted Forensics Evidence Using Blockchain. pp.57-61. 10.1145/3219788.3219792.

[9] M. Pourvahab and G. Ekbatanifard, "An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology," in IEEE Access, vol. 7, pp. 99573-99588, 2019.

[10] D. Le, H. Meng, L. Su, S. L. Yeo and V. Thing, "BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy," TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, Korea (South), 2018, pp. 2372-2377.

[11] M. Hossain, R. Hasan and S. Zawoad, "Probe-IoT: A public digital ledger based forensic investigation framework for IoT," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, 2018, pp. 1-2.

[12] Y. Zhang, S. Wu, B. Jin and J. Du, "A blockchain-based process provenance for cloud forensics," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, 2017, pp. 2470-2473.

[13] Infura. Available: https://infura.io/. [Online Accessed April, 2020].

[14] Web3.js. Available: https://web3js.readthedocs.io/en/v1.2.6/. [Online Accessed April, 2020]

[15] D. Ongaro, & J. Ousterhout (2013). In search of an understandable consensus algorithm (extended version).

[16] D. Fakhri, & K. Mutijarsa (2018, October). Secure IoT communication using blockchain technology. In 2018 International Symposium on Electronics and Smart Devices (ISESD) (pp. 1-6). IEEE.

[17] X. Burri, E. Casey, T. Bollé, & D. O. Jaquet-Chiffelle (2020). Chronological independently verifiable electronic chain of custody ledger using blockchain technology. Forensic Science International: Digital Investigation, 300976.

[18] D. O. Jaquet-Chiffelle, E. Casey, & J. Bourquenoud (2020). Tamperproof timestamped provenance ledger using blockchain technology. Forensic Science International: Digital Investigation, 300977.