ISSN 2063-5346

B-CoC: A BLOCKCHAIN-BASED CHAIN OF CUSTODY FOR DIGITAL FORENSIC INVESTIGATIONS

Febin Prakash*

School of Computer Application, CT University, Punjab, India.

Corresponding Author Email: vc@ctuniversity.in

Dr. Harsh Sadawarti

School of Computer Application, CT University, Punjab, India.

Email: febin18002@ctuniversity.in

Article History: Received: 12.06.2023 **Revised:** 14.07.2023 **Accepted:** 31.07.2023

ABSTRACT

In today's E-world, with the rapid rise in cybercrimes, the importance of digital evidence is also growing for the provenance of person linkage with cybercrimes. Digital evidence comes with its exclusive challenges related to the Chain of custody(CoC). CoC can be defined as a procedure to preserve and record the sequential history of handling digital evidence. With the advancement of technology, the preservation of digital evidence also becomes progressively more important in investigations. To maintain the authenticity and privacy of evidence, its entire lifecycle must be recorded. Also, traditional database technologies cannot preserve the integrity and authenticity of digital evidence. Blockchain-Based Chain of Custody is a blockchain-based answer for maintaining and tracing the digital forensics chain of custody. Blockchain is a data structure that permits creating a digital ledger for recording and storing transactions shared by all participating partners over a distributed networks. Blockchain makes use of cryptography for safeguarding the process of recording and keeping transactions that happen within the network, creating an unimpeachable audit trail. To achieve authentication, integrity, and confidentiality of digital evidence, in this research, we proposed using a blockchain-based chain of custody that can be used for forensic applications to bring in integrity and manipulate resistance to the digital forensics chain of custody.

KEYWORDS: Blockchain, Forensics, Chain of Custody, Digital evidence, Cyber Forensic.

INTRODUCTION

One of the main problems in digital forensics is the management of evidence. From the point of evidence collection until the time of their exploitation in a legal court, evidence may be accessed by multiple parties involved in the investigation that takes its ownership temporarily. The Chain of Custody(CoC) is the process of validating how any kind of evidence has been gathered, traced and protected on its way to a court of law. Chain

of Custody is not a mandatory step in forensic analysis[1]. However, it is extensively used as evidence; to be acceptable in a court or in legal procedures, it must be proved to be not tampered during investigation process. Thus, a good Chain of custody process should use a standard for dealing and handling evidence, irrespective of whether the evidence will be used in a trial or not.Currently, Chain of custody process requirements is met by employing a physical handover of evidence where, at each step, CoC forms are filled in and signed in front of case officers. In this form, we take a step toward the dematerialization of this process by proposing a Blockchain-based architecture for CoC of digital evidence called B-CoC. Leveraging the features offered by blockchain technologies, we defined an architecture able to support the CoC process[2]. To this aim, we proposed an architecture, namely B-CoC, that is able to realize an Evidence log with integrity checks (i.e., every process is able to verify and detect if there has been an integrity breach that would invalidate the digital evidence). B-CoC integrates together an ordinary database with a permissioned blockchain: the first represents the Evidence DB where digital evidence is stored, while the second represents the Evidence Log that allows for tracking digital evidence during their lifecycle. This distinction is made to store each type of information in the most suited kind of distributed storage: digital evidence are a relatively static and significant piece of information and do not need particular support for updates, while the evidence log is characterized by a reduced size of record to be stored and is subjected to a high update frequency. In particular, we set up a classified permission blockchain, and we applied an intelligent contract to keep track of the possession changes during the evidence lifecycle. We implemented our prototype on an Ethereum[3] private network, and we evaluated the impact of the system configuration parameters on performance.

A blockchain is basically a block of chains, with the growing list of entries referred to as blocks that are merged with cryptography [4]. Each blockchain contains a hash value of a previous block and a timestamp that keeps track of the creation and modification time of the file. In terms of security, not a single person not even the proprietors of the document, nobody able to modify once it has been recorded[17]. Blockchain was developed in 2008, and it was employed in 2009 to function in the general public dealings' ledger of the cryptocurrency, a type of electronic money[18]. Blockchain technology is decentralized that means peer-to-peer. It consists of network computers, which apply blockchain technology to put all together and manage the information that records each bitcoin dealing collected by its network[5]. The architecture of the blockchain technology demonstrated in Figure 1, executes a decentralized, fully replicated append-only ledger in a peer-to-peer network, initially employed for the bitcoin cryptocurrency.

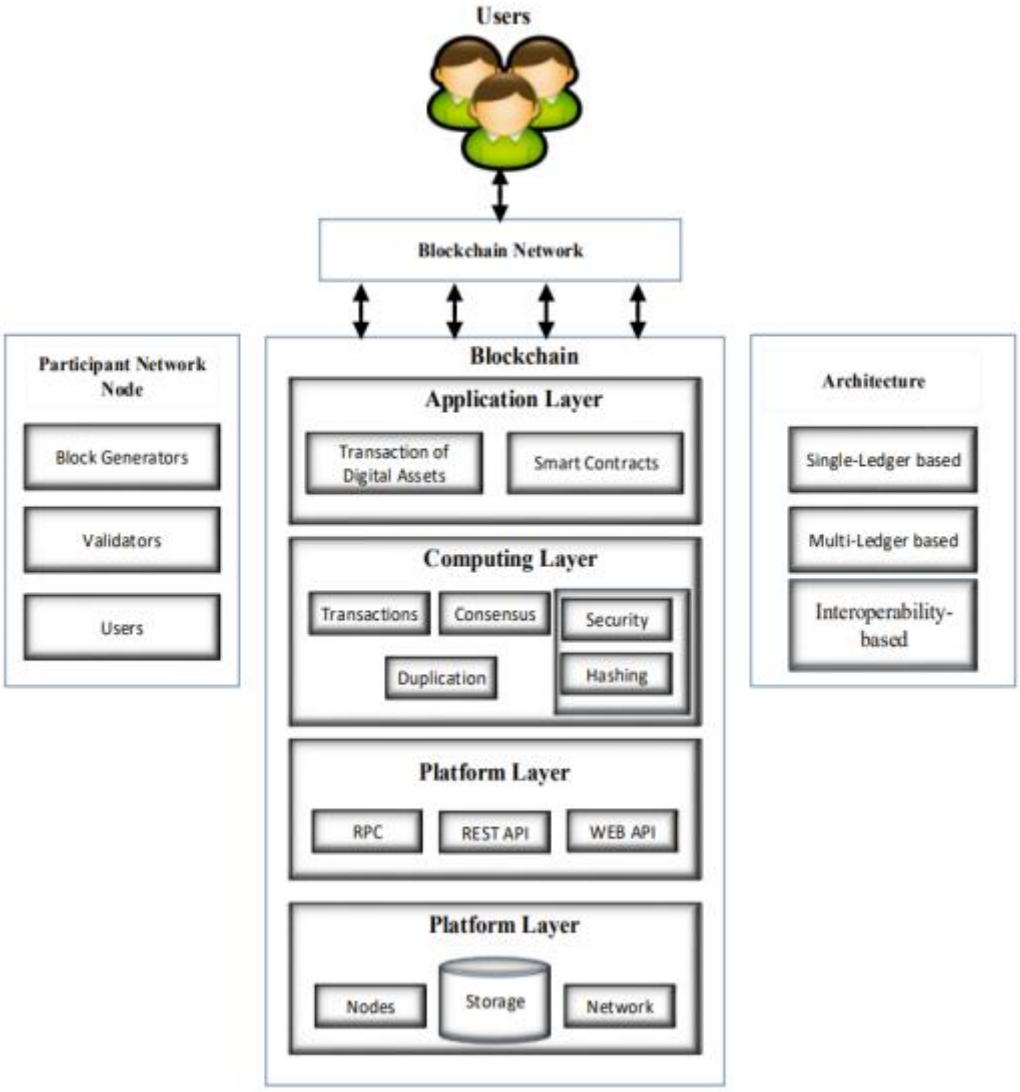

Figure 1. The architecture of blockchain[16].

Problem Analysis and Motivation

The crime investigation process relies deeply on physical and digital evidence nowadays. The judicial system allover the world has gradually become flexible in accepting digital evidence, given the fact that the digital evidence handling mechanism is somewhat similar to how they treat physical evidence. The field of digital crime investigation continues to grow rapidly and therefore requires adequate computer investigators with skills needed to capture the relevant evidence like crime scene, call data records, search collected records, recover data etc. and engage with the forensic process[6].

The issues a forensics investigation team encounters with digital evidence are due to the nature of digital information, which can be as follows:

• Easily duplicated

• Integrity of the evidence

• Accessibility to evidence

• Secure storing of evidence

• Transmitted to someone else or to a different country;

• In some cases, the digital evidence is time-sensitive to the case and pre-arrest situations.

An issue arises with the gap introduced when providing digital evidence versus physical in the court of law. This is undoubtedly becoming a challenge to the judicial system's solid and secure digital witnesses. Another issue is that there are different practices of digital forensics investigation models. Figure 2 illustrates the construct in the investigation process and how physical and digital evidence supports each other in creating a comprehensive theory about the criminal case[7].

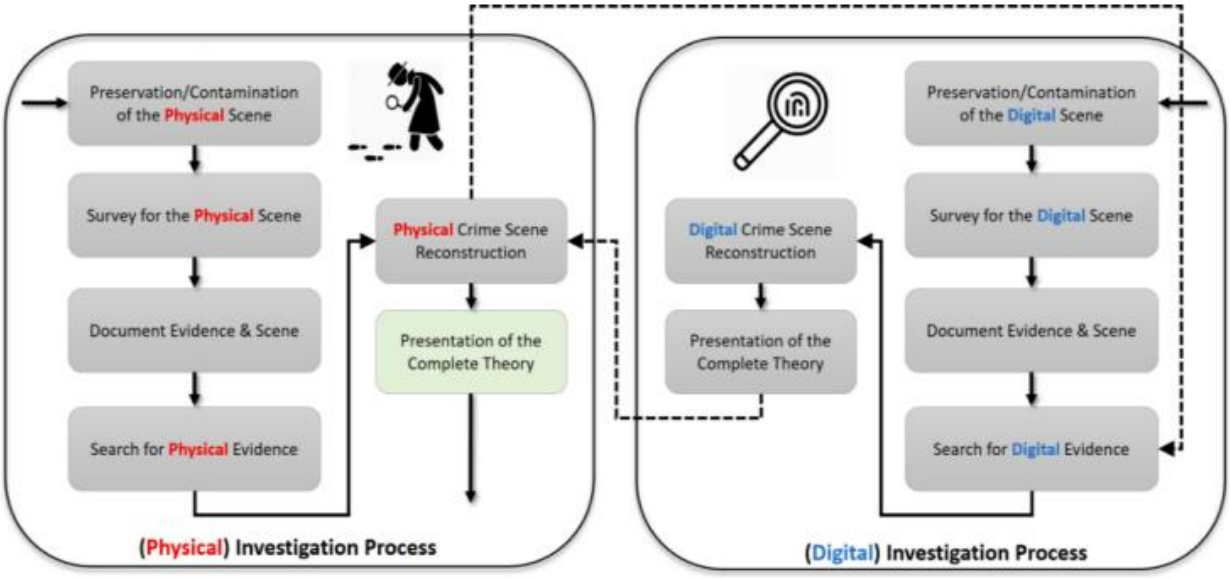

Figure 2. Physical and digital investigation constructs.

The paper explores for the utilization of blockchain technology to improve the Chain of custody(CoC) method and the evidence handling life cycle. The blockchain is a digital ledger system, namely distributed ledger technology, and we trust it can address the current issues challenged with the digital evidence-handling life cycle. distributed ledger technology (DLT) implementation is increasing as regards its benefits in improving sustainability, automation, and digital revolution. It also provides built-in security to control access to data and trace changes during the course of the data life period. However, the blockchain is an emerging technological improvement; hence very few solid, real-life applications are found.

The paper proposes a conceptual blockchain model, i.e., CB, to fill the gap in the literature and address the challenges faced in handling digital evidence to transform the global law practice efficiently. The conceptual blockchain model (CB) demonstrates how blockchain and smart contracts can provide scrutinized and traceable access to the evidence chain of custody for those involved participants, e.g., regulators, courts, law firms, etc. The conceptual blockchain model (CB) nodes are trusted network stakeholders with a viable and distributed set of rules/standards. The conceptual blockchain model (CB) intelligent contracts ensure the automation of rights on the evidence associated to the plaintiff, defendant, and involved third party. It also has the elasticity to adapt to and comply with the applicable juridical system and provide compliance metrics to the evidence handling lifecycle

Proposed B-CoC Model

B-CoC is a blockchain-based solution for maintaining and tracing the digital forensics chain of custody. Blockchain is a data structure that allows the creation of a digital ledger for recording and storing transactions (events/records) shared by all contributing parties over a widly spread network of computers. Blockchain makes use of cryptography for safeguarding the method of recording and storing transactions (events/records) that occur within the network, creating an unimpeachable audit trail[8]. In relation to the Chain of custody(CoC), the blockchain's capability, exclusively in combination with cryptographic hashing and encryption, could hypothetically create documentation pertaining to access to evidence that is tamper-proof . The evidence that is to be well-preserved is first encrypted securely and have a blockchain ability added on[9]. The encrypted data would be available only to the desired party on the blockchain network but would concurrently record the time, date and possibly user ID of the accessing party and add it to the irreversible record in blockchain, all done automatically through a smart contract. The blockchain itself can be read via a particular function in a way that is like how the bitcoin blockchain can be decoded. This functionality of blockchain allows courts and associated personnel the ability to examine the historical Chain of custody without accessing data itself[10].

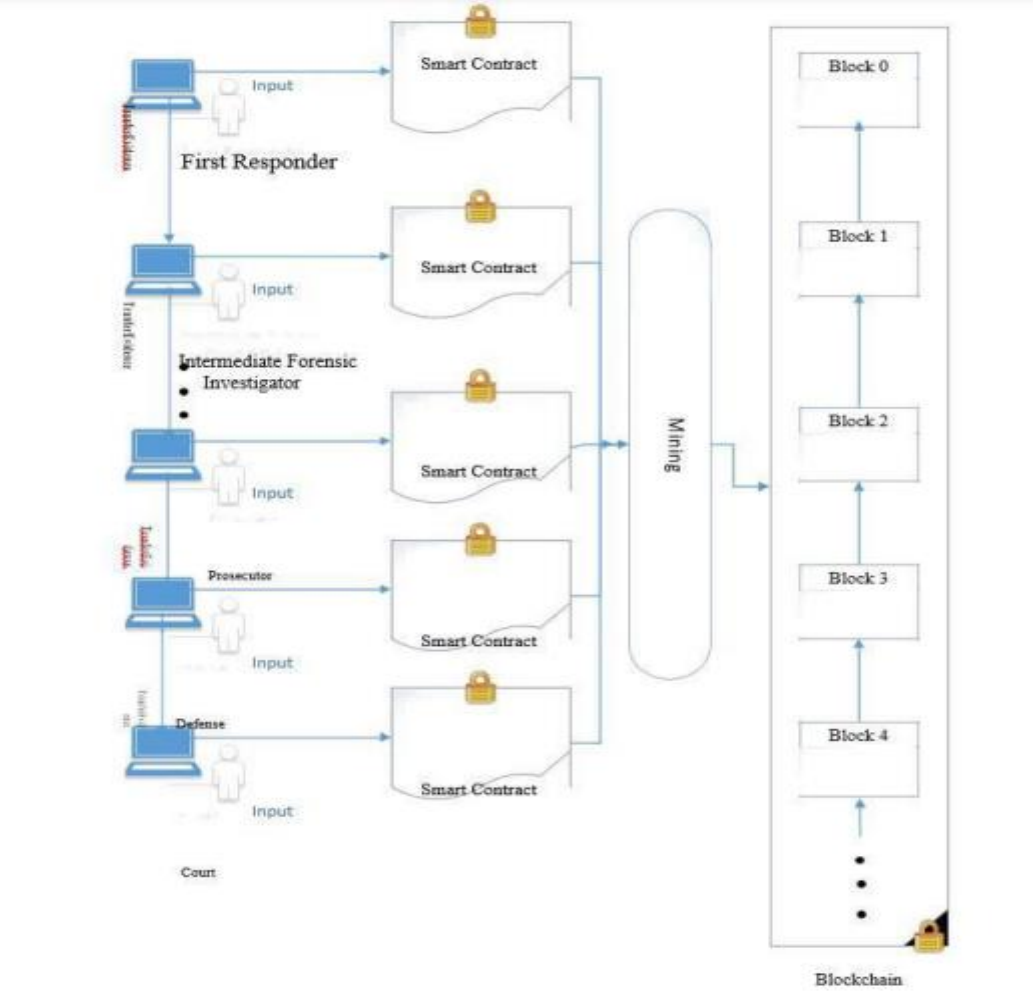

Figure 3. Blockchain based CoC

Benefits of Proposed Model

B-CoC: Blockchain-based digital forensics chain of custody has excellent potential to bring substantial benefits to forensic applications by maintaining integrity, transparency, authenticity, security and auditability of digital evidence to achieve the desired end[11]. Some of the benefits are summarized below:

- Collecting, preserving, and validating digital evidence can be strengthened with the help of B-CoC.
- The provenance of any action or event can be traced back to where it initially entered the process in question[12].
- B-CoC also helps in improving transactional efficiency and cost reduction of certain kinds of transactions due to increased transparency resulting in eliminating the requirement of a trusted third party for validation of specific claims or evidence transfer and consensus-based Proof of Trust, resulting in increased trust among communicating parties[13].
- Reduction of fraud due to improved transparency of the audit trail.
- B-CoC allows organizations to embed verification for the event or action within the evidence
- Record itself, thereby enabling established and ongoing evidence that is both accessible verifiable.

CONCLUSION

This paper presented B-CoC, a blockchain-based architecture to dematerialize the CoC process in digital forensics. Blockchain by design enforces integrity, transparency, authenticity, security and auditability, thus making it possibly the best choice for maintaining and tracing the forensic CoC. Blockchain help out in friction reduction through increased trust and thus brings real promise for the forensic community. The future work aims at developing a complete Ethereum based intelligent digital forensic Chain of custody using smart contracts.

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 March, 2022]. Web3.js. Available: https://web3js.readthedocs.io/en/v1.2.6/. [Online Accessed March, 2022]
14. D. Ongaro, & J. Ousterhout (2013). In search of an understandable consensus algorithm (extended version).
15. 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.
16. 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.
17. D. O. Jaquet-Chiffelle, E. Casey, & J. Bourquenoud (2020). Tamperproof timestamped provenance ledger using blockchain technology. Forensic Science International: Digital Investigation, 300977.