Egyptian Journal of
Forensic Sciences

REVIEW Open Access

Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework

Harsh Patil[1], Ravshish Kaur Kohli[1], Sorabh Puri[2] and Pooja Puri[1*]

Abstract

Background Proper investigation of digital evidence is of prime significance in cyber investigations. From the collection of evidence, its preservation, and its analysis, it is important to maintain its integrity in the legal system due to the involvement of different stakeholders like law enforcement agencies, digital analysts, and the judiciary. This review paper focuses on how blockchain technology can be used to collect evidence efficiently.

Main text In the present scenario, the manual logs of the chain of custody are used to ensure that the evidence remains confidential and transparent. It is accompanied by filling out the application forms and maintaining logs within the organization handling the evidence. Hence, it is important to ensure the validity, integrity, and verifiability of evidence as it moves through different hierarchical levels. There are certain issues associated with the current chain of custody, such as evidence loss, theft, tampering, and, even worse, evidence manipulation inside the system. To avoid this situation and to make the process coherent, this review paper aims to highlight the potential use of blockchain technology to preserve chain of custody.

Conclusion Although this scientific technology is mainly used to run cryptocurrencies, with careful consideration and application, this could play a key role in supporting and managing the chain of custody. It is a distributed database that keeps track of blocks. These blocks are collection of entries that keep growing continually and are secured from editing and manipulation by retaining the hash of the previous block in the chain. This is a decentralized technology that is not easily compromised in terms of security and therefore has the potential to solve our problem area. A future research agenda needs to be established, which lays the solid foundation for further studies on this evident emerging area.

Keywords Blockchain, Chain of custody, Cyber security, Digital evidence, Decentralized technology, Encryption

Background

In the legal system, evidence is utilized to convict a person or prove his or her innocence. Therefore, it is critical that the evidence's integrity and transparency must be proven in court. Evidence collection should preserve three basic security properties: authenticity, reliability, and refutation to ensure the admissibility of the associated evidence in a court of law (Ahmad et al. 2020).

With the rapid development in cybercrime in today's digital environment, the necessity of digital evidence for the traceability of persons linked to cybercrime is expanding. Digital evidence has its own set of issues in terms of the chain of custody (Lone and Naaz 2017).

Digital evidence, or any evidence for that matter, must pass through multiple divisions on its way from the crime scene to the courtroom. To secure the security properties, a chain of custody (CoC) is used to monitor

*Correspondence:
Pooja Puri
pmalik1@amity.edu
[1] Amity Institute of Forensic Sciences, Amity University, Sector 125, Noida, Uttar Pradesh 201301, India
[2] NSI, Orange Business Services, Gurugram, India

and document the chronological history of the evidence (Giova 2011). In the present scenario, the chain of custody (CoC) is maintained by keeping a logbook with records of the names of agencies that handle the evidence, which is a time-consuming and complicated method and often prone to tampering with evidence.

Blockchain is an innovative, decentralized, and distributive solution to our predicament. Blockchain technology, which promises to improve data security, privacy, and dependability, has recently piqued the curiosity of academics and policymakers. For transactions between multiple agencies, blockchain enables distributed and immutable ledgers, tamper-proof records, and built-in cryptographic capability (Valjarevic and Venter 2013).

Blockchain is a decentralized, immutable ledger that facilitates the tracking of assets and the recording of transactions within a network of an organization. In our case, assets refer to the evidence. The blockchain is an extensive chain of blocks that are linked together using cryptographic techniques that make tampering practically a challenge (Liu and Seo 2018).

Blockchain is usually a lengthy chain of data packets, called Blocks. Every single block is made up of several transactions. Each new block contributes to the blockchain, which is a complete log of transaction history (Billard 2018; Prayudi 2015). Blocks can be confirmed by the network using cryptographic techniques. Along with the transactions, each block also contains a timestamp, nonce, and hash value. The hash value of each block's parent block and the entities link them together. This procedure contributes to the integrity of the blockchain by utilizing the Genesis block (the first block in the chain). The hash value is a one-of-a-kind integer that serves as the block's unique identifier (Ritzdorf and Soriente 2018).

The method of committing a crime has evolved over time. If we investigate the ratio of cybercrime to conventional crimes, the rate of cybercrime is rising exponentially across the world. The cause of this has to do with the increase in electronic gadgets and digitalization of practically everything, whether it is processing online payments through multiple portals or accessing one's government id (Tziakouris 2018). Block DEF is based on a blockchain-based safe and scalable digital evidence architecture (Tian et al. 2019). The solution stores the evidence on a safe platform, and the data related to the evidence is kept in the blockchain. This architecture, which combines an effective name-based byzantine fault-tolerant consensus algorithm with a mixed block format, uses a lightweight blockchain (Cebe and Erdin 2018). The service layer, blockchain layer, and network layer are the three layers that makeup Block-DEF. Evidence-related services are included in the service layer, blockchain-related services and consensus protocols are included in the blockchain layer, and peer-to-peer networking is the foundation of the network layer. Block-DEF uses a multi-signature approach that uses random keys and certificated key pairs to maintain privacy and traceability (Montasari and Jahankhani 2020).

Bonomi et al. demonstrated a blockchain-based chain of custody (B-CoC) that is entirely based on a private and permission blockchain. This was decided in accordance with the CoC procedure, which prohibits unlicensed and unknown parties from managing evidence. Three parts make up B-CoC: the evidence database (a database containing digital evidence), the evidence log (which contains information on CoC and hashes on evidence), and the front-end interface (which serves as B-CoC's user interface). The blockchain-based evidence log includes details like the evidence ID, the evidence description, the identity of the originator, and the ownership history (Li et al. 2019). The court's chief coordinator and lightweight entities (such as forensic investigators) make up the peer-to-peer network on which the evidence log is based. The implementation process for evidence logs is broken down into three stages: the private blockchain, the private network, and finally the creation and deployment of smart contracts on top of the blockchain architecture (Lone Hamid and Mir 2017).

Billard et al. demonstrated that digital evidence is maintained in a blockchain, which retains the evidence's information and is available to all licensed participating parties. To enable relevant parties to assess the certainty and relevance of digital evidence, an external data structure called Forensics Confidence Rating is utilized. The Global Digital Timeline is another data structure offered, and it is used to hold the chain of events connected to digital evidence (Mezzour et al. 2018).

Ahmad et al. reviewed the use of blockchain-based smart locks for physical evidence, which will be merged via smart contract with a second blockchain that will include the evidence's metadata. The paper blockchain is built on top of the Ethereum blockchain. Ethereum is a decentralized, open-source blockchain platform that enables developers to build and deploy smart contracts and decentralized applications (DApps). It was proposed by Vitalik Buterin in late 2013 and development began in early 2014, with the network officially launching on July 30, 2015. Moreover, Ethereum introduced the concept of smart contracts, which are self-executing contracts with the terms of the agreement directly written into code (Lone Hamid and Mir 2017). It splits the frame into 3 layers: (1) Evidence Layer, blockchain-based smart locks; (2) Blockchain Layer, blockchain-based private Ethereum fork; and (3) Network Layer, peer-to-peer communication. As compared to alternative consensus algorithm implementations, preliminary evaluation of this research results demonstrates that the proposed framework can handle realistic workloads while maintaining an acceptable transaction throughput. By documenting the chain of custody on an immutable network, blockchain protects the integrity of evidence content and its admissibility in court (Paradise 2017).

Burri et al. proposed a method for timestamping hash values of evidence using an e-COC ledger administered by a trustworthy organization. The gathering of evidence should be carried out carefully in accordance with written SOPs or manuals. CoC ledger employs blockchain technology to prevent unauthorized changes. Moreover, certain blocks are put into a secure public blockchain to mitigate the impact of a hypothetical change to one block of the e-CoC ledger, because the public blockchain ledger is unalterable (Zou et al. 2019).

Prayudi et al. examined the issues encountered in the digital chain of custody as well as the efforts of scholars in giving solutions to these problems from diverse perspectives. There are still several issues that must be addressed before the digital chain of custody solutions can effectively act as an aggregation mechanism for processing evidence that will help law enforcement investigations (Zhao 2019).

Main text

Lifecycle of digital evidence

The gathering of evidence should be carried out carefully in accordance with written standard operating procedures (SOPs) or laboratory manuals. Unfortunately, in many instances, it is not followed in forensic investigations. In terms of who first comes into correspondence with digital proof, the situation varies by country (Kumar 2021). There are specialized units (first reaction forces) that are taught how to operate with this type of evidence, whereas in some nations, this work is performed by law enforcement personnel who do not have qualified degrees but attained specialized training (Cosic and Cosic 2012). The life cycle of digital evidence is extremely complicated, and it is extremely vulnerable to tampering throughout the entire cycle, from the crime location to the courtroom. The following individuals may come into touch with the evidence:

- Law enforcement officers
- Forensic experts
- Suspects
- Victims
- Eyewitness
- Media personnel

The first stage in the life cycle of digital evidence is identification and collection. The exhibits are either collected by first responders or by forensic investigators, depending on the nation's laboratory protocol (Wang and Wang 2018). The main goal is for an investigator to gather as much useful evidence as possible. It is a complex and difficult process to separate the relevant evidence from the irrelevant evidence. Then, the examination of evidence in forensic science laboratories. During this stage of the lifecycle, evidence encounters the forensic examiner. This is the point at which forensically significant data is extracted from vast amounts of digital data.

The third step is to prepare and present the report. This stage lists the approaches, techniques, and so on that were adopted to conduct the evidence analysis as well as the outcomes obtained after implementing them. The report is subsequently presented in court and examined by the prosecutor. Between these points, storage and transport always take place, and the chain of custody must always be maintained. After the case has been concluded or opened by the court and a verdict is issued, the evidence is maintained and archived by labs and the court, depending on their regulations (Shah and Ganesan 2019).

The third step is to prepare and present the report. This stage lists the approaches, techniques, and so on that were adopted to conduct the evidence analysis, as well as the outcomes obtained after implementing them. The report is subsequently presented in court and examined by the prosecutor. Between these points, storage and transport always take place, and the chain of custody must always be maintained. After the case has been concluded or opened by the court and a verdict is issued, the evidence is maintained and archived by labs and the court, depending on their regulations (Shah and Ganesan 2019).

Chain of custody

The chain of custody is a fundamental and critical process in the legal system, particularly in criminal and civil law cases. It refers to the chronological documentation and tracking of physical evidence from the moment it is collected at a crime scene or discovered through an investigation, through its handling, storage, and presentation in court. Typically, the chain of custody involves detailed records, including the names of individuals who had custody of the evidence, the dates and times of transfers, descriptions of the evidence, and any relevant information about its storage conditions (D'Anna 2023). The fact of the matter is that after evidence is gathered, the transfer of the evidence among all entities must be documented for the evidence to be acknowledged. Additionally, it must be demonstrated that the chain of custody is reliable. Nobody can acquire evidence unless the chain of custody is documented. And no one can alter the chain of custody record. If we can show that there are discrepancies in the chain of custody, the court will throw out all the evidence (Yan and Shen 2020).

In a court of law, physical and digital evidence are used in tandem to establish whether something is true or untrue. As a result, we might conclude that managing both physical and digital evidence is critical. Figure 1 depicts both physical and digital evidence that will aid in forensic activities.

The present system of maintaining the chain of custody consists of the accompanying agency filling out forms and putting them in a forensic lab or forwarding them to the prosecutor as well as keeping a logbook with all the documentation. The issue arises here because, in many circumstances, the chain of custody is taken for granted by a few policemen, scientific personnel, or any other authorized entity through which evidence transits throughout its life cycle. To strengthen the case in court, the conditions outlined in the chain of custody must be met.

- *Trustworthy*: The chain of custody should be sufficiently reliable for the court that it cannot be called into question. The agency involved in the process should ensure that the proper SOPs and procedures are followed throughout the process's life cycle.
- *Auditable*: At any point in time, the chain of custody should be auditable. It should be kept as transparent as possible. Every entity involved in the process must be able to verify the entire process.
- *Traceable*: The evidence must be tracked from its collection to its examination.
- *Tamper-proof*: The evidence should be kept secure and without any hindrance.
- *Integrity*: The evidence's integrity and confidentiality should be preserved, which means it should not have been altered or corrupted during the transfer.

Challenges to chain of custody

Blockchain technology has shown to have enormous potential for reducing scalability- and transparency-required traditional validation procedures. There are certain challenges to chain of custody which are as follows:

- *Excessive paperwork*: In the current scenario in India, an exhibit transfer between different agencies involves far too much paperwork, which includes the name of the agency accompanying the evidence, case number, transport permit, condition of evidence, name of person with evidence, time, integrity of stamp, and so on, consuming a significant amount

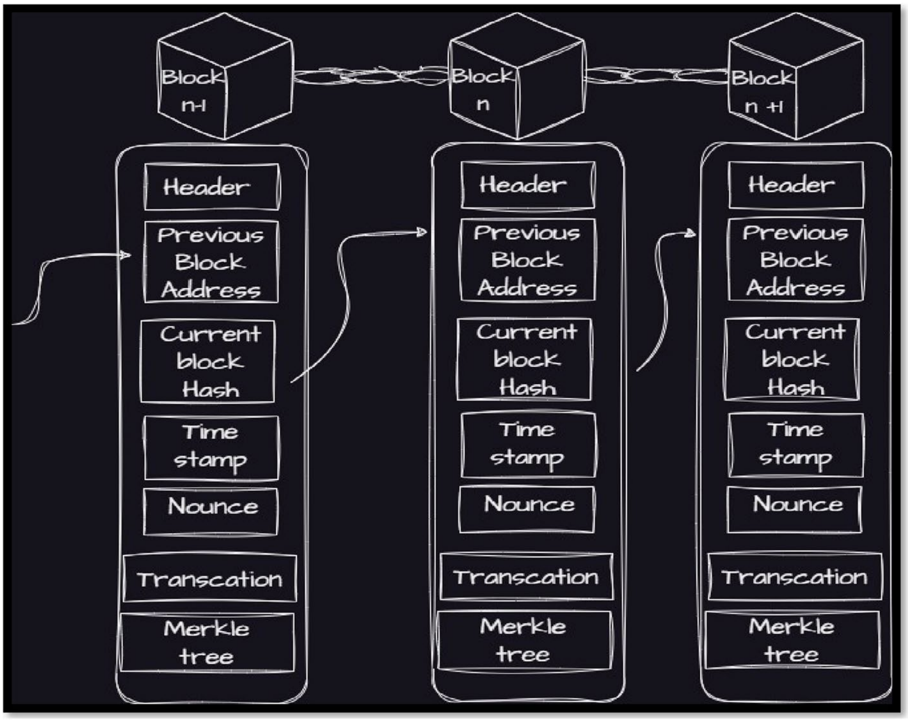

Fig. 1 Structure of blockchain

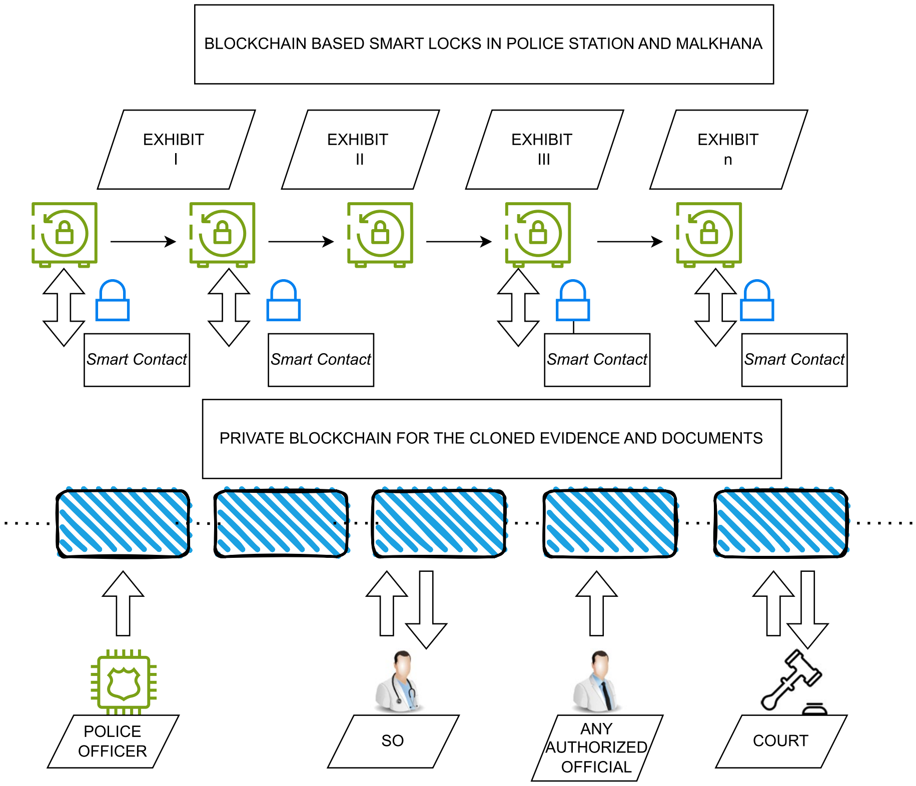

Fig. 2 Framework of blockchain-based CoC

of time. Acceptance of evidence for examination in a forensic science lab (FSL) might take up to a day.

- *Tampering/contamination potential*: The possibility of tampering with evidence is always significant, and numerous incidents have been documented in which either the evidence was contaminated or interfered with during the transfer of evidence from one agency to another and the record was clear in the chain of custody. The issue could be understood with the help of Fig. 2 by considering the case in the figure, where digital evidence was retrieved from the crime scene and was meant to be sent to the FSL, but the data on a storage device was tampered with by the first responder and then submitted to the FSL for assessment.
- *Justifying the chain's integrity in court*: The requirement that a piece of evidence be proven to be genuine, that is what its presenter claims it to be, is referred to as authentication or identification of true evidence. To achieve this, the chain of custody's integrity must be proven in a high court of law (Giannelli 1996). This is the most critical challenge to the current system for maintaining chain of custody, as any minor flaw by the first responder or other agencies is enough for the defense to hinder the court, resulting in the case being dismissed and the suspect walking free from court even if he or she is guilty.
- *Tracking interaction with exhibits*: Tracking down who had contact with the evidence when it was transferred to labs from a police station, or a crime scene is difficult to trust since the individual indicated on record may become antagonistic and tamper with the evidence.

Blockchain in the maintenance of chain of custody

In this section, we will cover our approach based on previous studies done in this domain, Information about the "BASE-64 Algorithm," as well as the blockchain as a service in the chain of custody and the advantages it offers.

- Blockchain as stakeholder: As previously stated, blockchain is a distributed ledger system that is highly encrypted, can be inspected at any point, and can avoid unauthorized access while retaining data integrity and confidentiality (Chopade and Khan 2019). Blockchains are classified into three types: public, private, and consortium blockchains. A public blockchain network is one in which anybody who is connected to the network may freely read and publish by using a private blockchain organizations may control who gets access to blockchain data, Certain data sets can only be viewed by those who have been granted authority (Zhang et al. 2021). The consensus process in a consortium blockchain network is carefully governed by a set number of nodes or stakeholders.

- Base64 encryption: Base64 is an encoding system for binary data that transforms it into ASCII text format. It organizes the data and expresses it exactly in 6 bits. The use of Base64 restricted. It uses an algorithm to translate binary data and can incorporate pictures, audio, and video assets in text format (Chopade and Khan 2019). The encoded textual data provides simple transmission over networks with no data loss. The first 62 values are from A to Z, a-z, and 0 to 9. The symbols + and / are also used. After processing with the Base64 technique, the combination of these 64 characters is utilized to build a hash value of the data as output.
- Framework of the blockchain-based CoC: In the framework, the first responder's major responsibility after collecting evidence from the crime scene is to protect the evidence, then capture volatile data and record down every detail such as the type of evidence, size, hash value, and so on. The digital forensic expert must clone the data of digital evidence because it is a fundamental principle of forensic science to never operate on the original digital exhibit. After the cloning process is completed, the case's IO will upload the cloned data to the blockchain, and the physical exhibit will be packed, sealed, photographed, and stored in the blockchain-based smart lock vault in the police station until the evidence is produced in court. The data can then be retrieved by authorized staff of the concerned entity who have been assigned to work on the evidence by inputting the case id and their private key on the chain (Bradford and Ray 2007).
- After the labs have evaluated the evidence, the court can use its private key and case id to access the details of the exhibit and swiftly inspect the lab results as well as verify the integrity and authenticity of the chain of custody.

Many other "blockchain based chain of custody" architectures have been proposed, including those by Lone and Naaz (2017); Bonomi et al. 2018; Burri and Casey 2020) who used Jakobsson algorithm to maintain chain of custody of digital evidence. In this section, we will use the architecture of the (Chopade and Khan 2019) to achieve our intended objectives. We create the architecture of the blockchain-based chain of custody, which is depicted in the Fig. 3.

Element 1—Evidence generation

This is a vital point because it is the first stage of the CoC. The sole person who can add evidence to the chain and create it is a police officer. He or she must enter every detail in the chain, such as the hash value generated from "BASE-64," time of collection, officer identity and rank, and many other details.

Element 2—Evidence transfer

The evidence is transferred to another authorized agency in this element, such as the police officer transferring the evidence to the scientific officer (S.O) for examination. So, to transfer the evidence, the participant needs to enter his/her details and the receiver's details, and then a hash will be generated. If in case any personnel tries to tamper with the evidence, the hash value of the current block and subsequent blocks will change, or anyone attempting to change the case ID or the evidence will be unable to do so for the same reason, thereby avoiding evidence and CoC tampering.

Element 3—Evidence display

Everyone on the network will be able to see the evidence. The first responder will generate the hash value of the evidence by using the BASE-64 algorithm and then upload it on the chain. Anyone on the chain whose details were entered for ownership transfer will decode the hash value to retrieve the actual evidence. The court can also be certain that the evidence was not tampered with at any point in its life cycle, allowing them to cross-check the authenticity by auditing the chain.

Disadvantages of blockchain

The blockchain network's high level of security is maintained by private keys. It is useful when validating a blockchain address. Furthermore, when you open a crypto wallet, you are given a private key. It is a password that permits you to take money out of your wallet. Blockchain technology is well-known for its superior security. There is, however, a gap in its armor that you should be aware of. The validation procedure in a blockchain is carried out by miners with a large amount of processing power. Implementing blockchain in a business is expensive. Most businesses are hesitant to engage in this technology because of the high cost of capital.

Utilization of blockchain in the court of law

A list of the evidence hashes from each case, along with the physical evidence put up for use in each case, will be

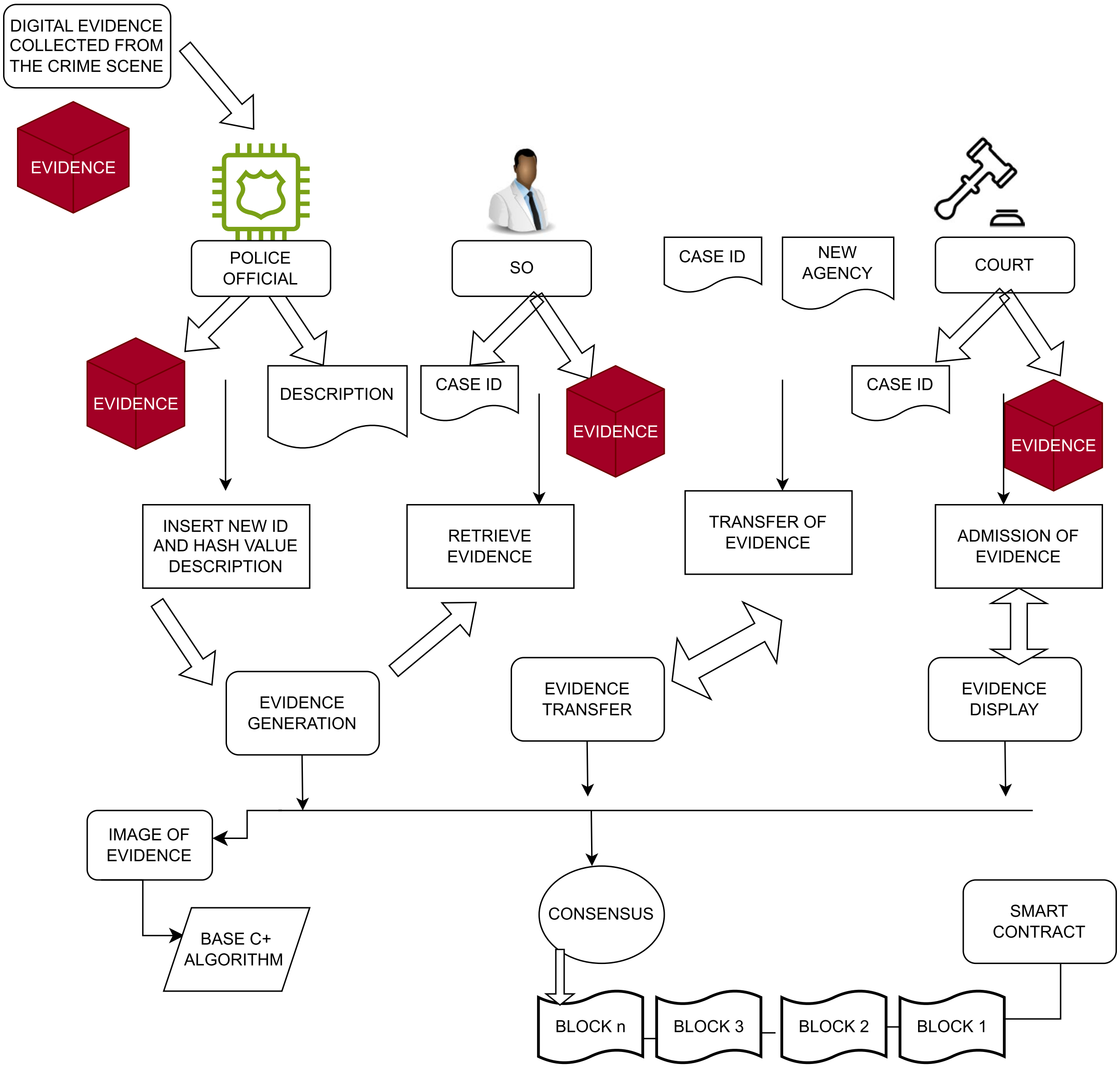

Fig. 3 Architecture of blockchain

made available to the prosecution, defense, and judicial authorities when blockchain is employed in a court environment. The blockchain will add integrity by strengthening the legitimacy of the evidence, which will further reinforce the argument. This will make it simpler for all parties to ascertain the truth and legitimacy of the case. As a result, it might speed up the judge's decision-making process and lessen the possibility of damaging or irrelevant evidence being accepted into the courtroom. Early dismissal of frivolous cases will result in a greater amount of evidence being proven relevant and valid, which will make less compelling evidence visible. Even better, it might be possible for the prosecution and the defense to agree in advance on the admissibility of the evidence, eliminating the need for some trials and the associated expenditures and backlogs. Because there is less room for human error with blockchain, this will guarantee that the justice system will be quicker, more reliable, and more secure. In a courtroom, a person accused of a crime would be able to check the integrity of the evidence and make sure nothing had changed by comparing a recent hash to the evidence gathered at the scene.

The application of blockchain technology in the chain of custody procedure has a number of potential benefits. It holds considerable promise for enhancing digital evidence handling and preservation, particularly in forensic investigations.

Conclusions

In this review paper, the chain of custody exists to ensure full transparency of the process of how evidence is collected, handled, and stored. Moreover, any kind of potential threat to digital evidence can be avoided with the help of blockchain. It is the perfect solution for maintaining and tracing chains of custody because it enforces integrity, transparency, authenticity, security, and auditability by design. By using blockchain technology with the chain of custody process, officials could greatly improve the process of ensuring all five of these criteria are met. Blockchain has become a trusted technology that is traceable through its blocks of data, which is vital when examining the historical chain of custody. Hence, there would be potential usage of blockchain technology in maintaining the integrity of evidence in the forensic field.

Future work

The future work will focus on the preservation of other evidence via a blockchain-based chain of custody as well as on training methods that can be used to upgrade the skills and knowledge of police officers and other law enforcement officials.

Abbreviations

CoC	Chain of custody
D.E.F.	Digital evidence framework
F.S.L.	Forensic science laboratory
S.O.	Scientific officer
S.O.P.	Standard operating procedures

Acknowledgements

The authors are grateful to the forensic experts and other scientific officers for communicating and providing valuable information for manuscript preparation.

Authors' contributions

HP—collected the review data and explored the significance of the study in the field of forensic science and drafted the manuscript; RK—drafted the manuscript and edited the review paper; SP—reviewed and rechecked the manuscript; PP—supervision, evaluation, and editing.

Funding

Not applicable.

Availability of data and materials

Not applicable.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

All authors have given the consent for manuscript publication.

Competing interests

The authors declare no competing interests.

Received: 30 June 2023 Accepted: 28 December 2023
Published online: 29 January 2024

References

Ahmad L, Khanji S, Iqbal F et al. (2020) Blockchain-based chain of custody: towards real-time tamper-proof evidence management in ACM International Conference Proceeding Series. AssocComput Machinery. https://doi.org/10.1145/3407023.3409199

Billard D. (2018) Weighted forensics evidence using blockchain. ACM International Conference Proceeding Series, Association for Computing Machinery: 57–61. https://doi.org/10.1145/3219788.3219792.

Bonomi S, Casini M, Ciccotelli C (2018) B-CoC: a blockchain-based chain of custody for evidences management in digital forensics. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12

Bradford PG, Ray DA (2007) Using digital chains of custody on constrained devices to verify evidence. IEEE International Conference on Intelligence and Security Informatics, ISI 2007, New Brunswick, New Jersey, pp 23–24

Burri X, Casey E (2020) Chronological independently verifiable electronic chain of custody ledger using blockchain technology. Forensic Sci Int Digit Investig 33.https://doi.org/10.1016/j.fsidi.2020.300976

Cebe M, Erdin E et al (2018) Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Commun Mag 56(10):50–57. https://doi.org/10.1109/MCOM.2018.1800137

Chopade M., Khan S (2019) Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE

Cosic J. and Cosic Z. (2012) Chain of custody and life cycle of digital evidence

D'Anna T (2023) The chain of custody in the modern era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data. Healthcare 11(5):634

Giannelli P. C (1996) Chain of custody. Law Scholarly Commons School of Law Scholarly Commons Faculty Publications

Giova G. (2011) Improving chain of custody in forensic investigation of electronic digital systems

Gulshan Kumar (2021) Internet-of-forensic (IOF): a blockchain based digital forensics framework for IOT applications, Future Generation Computer Systems. vol:120

Li S, Zhao S, Yang P, Andriotis P, Xu L et al (2019) Distributed consensus algorithm for events detection in cyber-physical systems. IEEE Internet Things J 6(2):2299–2308. https://doi.org/10.1109/JIOT.2019.2906157

Liu Z, Seo H (2018) IoT-NUMS: evaluating NUMS elliptic curve cryptography for IoT platforms. IEEE Trans Inf Forensics Secur 14(3):720–729. https://doi.org/10.1109/TIFS.2018.2856123

Lone H. and Naaz R. (2017) Forensic-chain: Ethereum blockchain based digital forensics chain of custody

Lone Hamid A, Mir RN (2017) Forensic-chain: Ethereum blockchain based digital forensics chain of custody. Sci Pract Cyber Secur J 1(2):21–27

Mezzour G. Frankenstein W. ley (2018) A socio-computational approach to predicting bioweapon proliferation. IEEE Trans Comput Soc Syst. 5(2):458–467. https://doi.org/10.1109/TCSS.2018.2813529

Montasari R, Jahankhani H et al (2020) Internet of things devices: digital forensic process and data reduction. Int J Electron Secur Digit Forensics 12(4):424–436. https://doi.org/10.1504/IJESDF.2020.110676

Paradise A (2017) Creation and management of social network honeypots for detecting targeted cyber attacks. IEEE Trans Comput Soc Syst 4(3):65–79. https://doi.org/10.1109/TCSS.2017.2719705

Prayudi Y (2015) Digital chain of custody: state of the art. Int J Comput Appl 114(5):1–9. https://doi.org/10.5120/19971-1856

Ritzdorf H, Soriente C et al (2018) Toward shared ownership in the cloud. IEEE Trans Inf Forensics Secur 13(12):3019–3034. https://doi.org/10.1109/TIFS.2018.2837648

Shah A, Ganesan R (2019) Understanding tradeoffs between throughput, quality, and cost of alert analysis in a CSOC. IEEE Trans Inf Forensics Secur 14(5):1155–1170. https://doi.org/10.1109/TIFS.2018.2871744

Tian Z, Li M, Qiu M, Sun Y, Su S (2019) Block-DEF: a secure digital evidence framework using blockchain. Inf Sci (n y) 491:151–165. https://doi.org/10.1016/j.ins.2019.04.011

Tziakouris G (2018) Cryptocurrencies - a forensic challenge or opportunity for law enforcement? An INTERPOL Perspective. IEEE Secur Priv 16(4):92–94. https://doi.org/10.1109/MSP.2018.3111243

Valjarevic A, Venter H (2013) A harmonized process model for digital forensic investigation readiness. IFIP Adv Inf Commun Technol 410(2):67–82. https://doi.org/10.1007/978-3-642-41148-9_5

Wang S, Wang X (2018) Parallel crime scene analysis based on ACP approach. IEEE Trans Comput Soc Syst 5(1):244–255. https://doi.org/10.1109/TCSS.2017.2782008

Yan W., Shen J (2020) Blockchain based digital evidence chain of custody. ACM International Conference Proceeding Series, Association for Computing Machinery, pp. 19–23. https://doi.org/10.1145/3390566.3391690

Zhang J, Hong Zhong, Chengjir Gu, Lu Liu (2021) Secure and efficient certificateless provable data possession for cloud-based data management systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 12681 LNCS. p. 71–87. https://doi.org/10.1007/978-3-030-73194-6_5

Zhao D (2019) Virus propagation and patch distribution in multiplex networks: modeling, analysis, and optimal allocation. IEEE Trans Inf Forensics Secur 14(7):1755–1767. https://doi.org/10.1109/TIFS.2018.2885254

Zou D et al (2019) A Multigranularity forensics and analysis method on privacy leakage in cloud environment. IEEE Internet Things J 6(2):1484–1494. https://doi.org/10.1109/JIOT.2018.2838569

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.