International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Blockchain - Based Digital Forensics Investigation

Dr. Deepika Sharma, Sakshi

[1, 2]Department of Computer Science & IT, Ramnagar Campus, University of Jammu, India
[1]*deepika. sharma231985[at]gmail.com*
[2]*sakshibhardwaj1208[at]gmail.com*

Abstract: ***Digital criminal investigation, each and every evidence whether it is collected from CCTV footage or by event data recorders are highly valuable. However, there may be risk when this digital evidence obtained during the investigation of a case is managed through a physical storage device. These evidences can easily be manipulated or destroyed before submitted in the court. Therefore, there is a need to reliably manage digital evidence and investigation using blockchain technology. The proposed Blockchain based Crime Investigation Method (BCIM) model is two phase blockchain model which separates the digital evidences into hot and cold block chains. The information that frequently changes is stored in the hot blockchain and the unchanging data such as videos, images are stored in the cold blockchain. Further in order to strengthen the proposed blockchain based model, the performance of digital crime evidence videos at different parameters can be measured.***

Keywords: Forensics, Blockchain, Crime investigation, Digital forensics

1. Introduction

Digital evidence plays an important role in cybercrime investigation, as it is used to link persons with criminal activities. Thus it is of extreme importance to guarantee integrity, authenticity, and auditability of digital evidence as it moves along different levels of hierarchy during a cybercrime investigation. Blockchain technology’s capability of enabling a comprehensive view of transactions whether events or actions, back to origination provides enormous promise for the forensic community. In this research, we proposed to use a blockchain - based system that can be leveraged for digital forensic investigation and its applications in particular bringing integrity and tamper resistance to digital forensics. The research primarily focuses on:

- The proposed system that deals with legal evidence (digital evidence) during criminal investigation using blockchain.
- Propose a two - level blockchain system that separates digital evidence into the hot and cold blockchain.
- For evaluating the system, we measure the storage and inquiry processing performance of digital crime evidence images and videos according to the different capacities in the two - level blockchain systems.
- The forensics field to investigate and preserve the evidence for the future and prevent them from being forged or tampered with.

2. Background

Different researchers study various methods and techniques of blockchain in the area of digital criminal forensics. This work provides a systematic literature review of blockchain - based applications across multiple domains. The aim is to investigate the current state of blockchain technology in the area of digital criminal forensics and its applications in various domains of crime evidence analysis [1].

Blockchain was first developed to support the well - known crypto currency Bit coin. Nakamoto proposed Bit coin in 2008 and implemented it in 2009 [2]. Since then, it has had tremendous growth in the stock market, reaching a value of $10 billion in 2016. A blockchain is a series of blocks that serve as a public ledger for all committed transactions. [3]. When fresh blocks are added to the chain, it continues to expand. Blockchain operates in a decentralized environment that is made possible by a combination of basic technologies like digital signatures, cryptographic hashes, and distributed consensus methods. All transactions are completed decentralized, removing the need for any intermediaries to confirm and verify the transactions. [4]. Decentralization, transparency, immutability, and auditability are some of the major aspects of blockchain [5]. Although Bit coin is the most well - known application of blockchain, it may be used for a variety of purposes other than crypto currencies. Blockchain applies to a variety of financial services, including digital assets, remittances, and online payments [6]. Blockchain technology has taken on a life of its own, infiltrating a wide spectrum of industries such as finance, healthcare, government, manufacturing, and distribution [7]. The blockchain has the potential to innovate and alter a wide range of applications, including products transfer (supply chain), digital media transmission (sale of art), remote service delivery (travel and tourism), platforms, and distributed credentialing. Distributed resources (electricity generation and distribution), crowd funding, electronic voting, identity management, and controlling public records are all examples of blockchain uses [8].

Digital cameras and mobile devices are frequently confiscated as evidence sources in forensic investigations. The video and photos retrieved from these devices are commonly employed in crime evidence investigations, as they can supply vital forensic evidence items, put together existing evidence pieces, and establish relationships between evidence items in a specific case. Closed - circuit television (CCTV) systems are commonly utilized in malls, banks, traffic junctions, stores, and even homes, where video evidence retrieved from these systems can be used as evidence much more than ever before. Audio and video evidence can be conveniently available in investigations when using smart devices such as a mobile phone, smart watch, and so on [9]. The scientific process of identifying, preserving, collecting, and presenting digital evidence so that it is admissible in a court of law is known as digital forensics. In reality, any information stored or extracted from digital media might be considered a piece of digital evidence that can be analyzed during a digital forensics inquiry [10]. Because the goal of any forensic investigation is to ensure that the digital evidence produced is acceptable in court, maintaining a chain of custody is a vital criterion that must be established throughout the investigation process [11]. With the increasing number of cybercrimes, the digital forensics team has no choice but to implement more robust and resilient evidence - handling mechanisms. Fahad F. Alruwaili proposed a unique method, which uses a conceptual blockchain paradigm [12]. Auqib and colleagues proposed that for ensuring integrity, transparency, authenticity, security, and auditability of digital evidence to reach the intended objective, blockchain - based digital forensics chain of custody has the potential to deliver significant benefits to forensic applications [13]. Renpeng Zou et al. suggested a blockchain - based photo forensics system that took into account copyright conflicts and photo tracing problems [14].

3. Methodology

Forensic Investigation tends to operate in regulated environments and requirements such as the identity of investigators who are investigating the crime - related cases. Digital forensics readiness is the ability of organizations to respond quickly and collect digital evidence related to a security incident with minimal cost or interruption to the ongoing business.

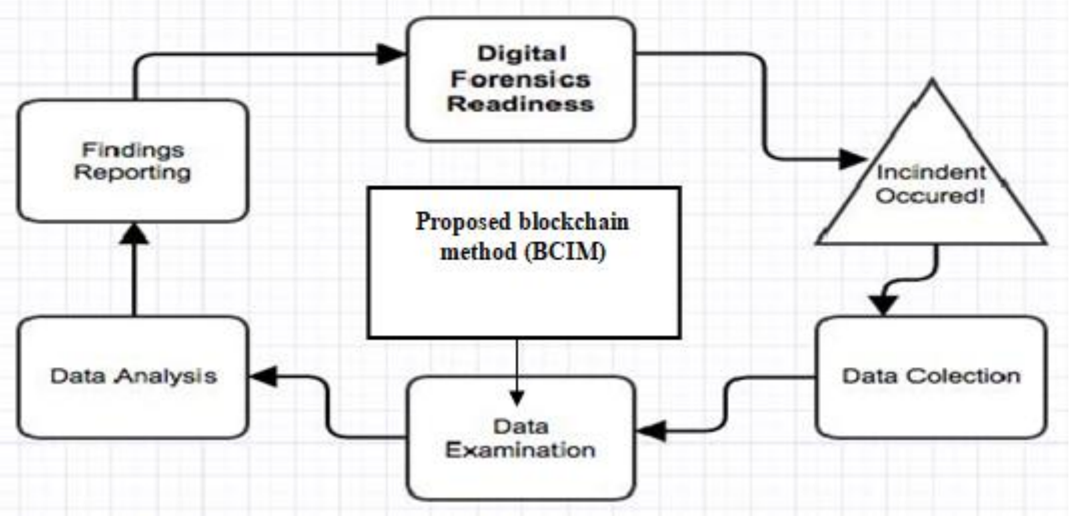

Figure 1.1: The workflow of the proposed criminal model using blockchain (BCIM)

This involves being able to define digital evidence required so that security aspects in an organization such as programs or teams and infrastructure can be adapted and modified to provide this evidence on time. In the course of operations, organizations generate a lot of digital data and records. Such data and records can become crucial pieces of evidence in the event of an unwanted incident. The data is being collected and examined.

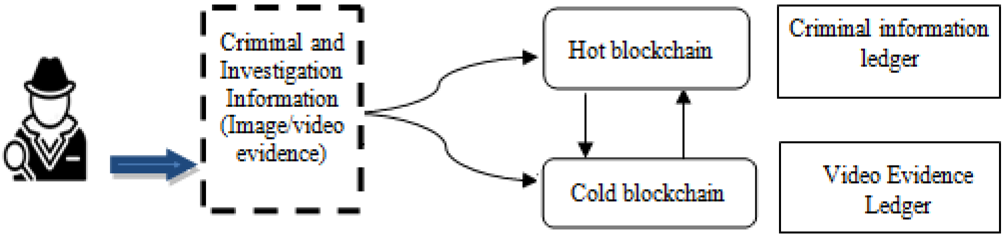
Criminal and Investigation Information (Image/video evidence)
Hot blockchain
Cold blockchain
Criminal information ledger
Video Evidence Ledger

Figure 1.2: Two - level blockchain system

Our proposed two level blockchain system is efficient for crime evidence management which consists of two layers, managed by hot and cold block chains (Fig 1.2). In the hot blockchain, investigation and identity information with frequent transaction fluctuations throughout the criminal investigation process is stored, and the cold blockchain stores digital crime evidence videos that do not require modification after storage. To evaluate the system, we measured the storage and inquiring processing performance of digital crime evidence videos according to the different capacities in the two level blockchain systems.

4. Discussion

The proposed two - level blockchain system increases the integrity of digital crime evidence, to efficiently manage criminal evidence. In the proposed system, only authorized participants can access the hot and cold block chains, in a decentralized environment to separate, store, and share the original information of the investigation, identity information, and digital crime evidence videos. The two - level blockchain system stores the investigation and identity information, as well as digital crime evidence videos, by on - site investigators with verified identities. Investigation and identity information, as well as digital crime evidence videos, once created in blocks, cannot be deleted by any user. In addition, because the block is shared with all institutions in the two - level blockchain system, transparency and reliability are enhanced.

References

[1] Casino, F., Dasaklis, T. K., & Patsakis, C “A systematic literature review of blockchain - based applications: current status, classification, and open issues, ” Telematics and Informatics. doi: 10.1016/j. tele.2018.11.006, 2018.

[2] S. Nakamoto et al., “Bitcoin: A Peer - to - Peer Electronic Cash System, ” Citeseer, 2008. [Online]. Available: http: //bitcoin. org/bitcoin. pdf

[3] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al - Fuqaha, ‘‘Blockchain for AI: Review and open research challenges, ’’ IEEE Access, vol.7, pp.10127–10149, 2019.

[4] A. Litke, D. Anagnostopoulos, and T. Varvarigou, ‘‘Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment, ’’ Logistics, vol.3, no.1, p.5, Jan.2019.

[5] M. Kouhizadeh and J. Sarkis, ‘‘Blockchain practices, potentials, and perspectives in greening supply chains, ’’ Sustainability, vol.10, no.10, p.3652, Oct.2018.

[6] G. Peters, E. Panayi, and A. Chapelle, ‘‘Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective, ’’ J. Financial Perspect., vol.3, no.3, pp.1–25, Nov.2015.

[7] J. Al - Jaroodi and N. Mohamed, ‘‘Blockchain industries: A survey, ’’ IEEE Access, vol.7, pp.36500–36515, 2019.

[8] Le, Tuan - Vinh & Hsu, Chien - Lung. (2021). A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges. Journal of Internet Technology.22.789 - 801.10.53106/160792642021072204007.

[9] J. Xiao, S. Li and Q. Xu, "Video - Based Evidence Analysis and Extraction in Digital Forensic Investigation, " in IEEE Access, vol.7, pp.55432 - 55442, 2019, doi: 10.1109/ACCESS.2019.2913648.

[10] Charan T S, K M Sowmyashree, 2021, Criminal Digital Forensic Investigation Application based on Blockchain, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 08 (August 2021)

[11] Auqib Hamid Lone, Roohie Naaz Mir, Forensic - chain: Blockchain - based digital forensics chain of custody with PoC in Hyperledger Composer, Digital Investigation, Volume 28, 2019, Pages 44 - 55, SSN 1742 - 2876,

[12] Alruwaili, Fahad F.2021. “CustodyBlock: A Distributed Chain of Custody Evidence Framework” *Information* 12, no.2: 88. https: //doi. org/10.3390/info12020088

[13] Lone, Auqib., “ Forensic - chain: Ethereum blockchain based digital forensics chain of custody, ” Scientific and practical cyber security journal.1.2017

[14] Zou, R., Lv, X., & Wang, B. “ Blockchain - based photo forensics with permissible transformations, ”. Comput. Secur., 87.2019

[15] S. Li, T. Qin and G. Min, "Blockchain - Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems, " in IEEE Transactions on Computational Social Systems, vol.6, no.6, pp.1433 - 1441, Dec.2019, doi: 10.1109/TCSS.2019.2927431.

[16] Kim, Donghyo, Sun - Young Ihm, and Yunsik Son.2021. "Two - Level Blockchain System for Digital Crime Evidence Management" *Sensors* 21, no.9: 3051. https: //doi. org/10.3390/s21093051

[17] Mercan, Suat & Cebe, Mumin & Aygun, Ramazan & Akkaya, Kemal & Toussaint, Elijah & Danko, Dominik. (2021). Blockchain - based video forensics and integrity verification framework for wireless Internet - of - Things devices.10.1002/spy2.143.