Blockchain Hyperledger Sawtooth Enabled Digital Forensics Chain of Custody (CoC): A Review

Tuba Mehmood, Uzaif Ahmed, Subhan
Department of CS&IT, Benazir Bhutto Shaheed University
Lyari, Karachi, Sindh 75660, Pakistan
tubamehmood948@gmail.com, uzaifahmed10101@gmail.com, subhankhatri31@gmail.com

Received: 21st July 2022; Accepted:29th December 2022; Published: 30th December 2022

Abstract: This project gives the architecture design and a complete understanding of the project" Blockchain Hyperledger Sawtooth Enabled Digital Forensics Chain of Custody" in this architecture design we have assign our own digital forensics engineer responsible for all the perquisite. This project is implemented to make the digital forensics Chain of Custody entire system in a decentralized environment in order to make the system free from corruption we have used smart contracts designed in the go language. We have used the concept of digital signatures and hash encrypted SHA256 function which would be widely expected to provide security and protection to digital forensics and chain of custody, as we know blockchain technology is rapidly evolving day by day, we will implement SHA-512 in future to make the system private for all the stakeholders. This project is developed to solve the problem of the investigation system, it will assist the people towards securing their data and evidence collection system that make forensic CoC more efficient than the previous system. for example, an accused is not allowed to know about investigators nor investigator is allow to see someone else details.

Keyword: Blockchain, Hyperledger Sawtooth, Digital forensics, Chain of custody (CoC), Smart contract; Consensus algorithm, Distributed application (Dapp).

I. INTRODUCTION

Digital forensics is a concept developed to preserve investigational material. we conclude from the keyword digital and forensics that it is a field that facilitates investigators to tackle technological corruptions. There is also a concept of digital evidence that is crucial, as it is a person that acts as a link between all crimes. Due to the security concerns, we are moving the chain of custody towards a blockchain hyperledger sawtooth framework that provides efficiency to the chain of Custody and make the system more advance and trustworthy In this project, our intention is to defend the data of every individual in court cases i.e., accuse, victim, digital investigator, and witnesses. In this work we give the architecture, in which we appoint our own digital forensics engineer he is authorized to do changes in a ledger he can begin the case by inserting evidence in the system he can control all the stakeholders in order, to make the system free of deception. Chain of custody (CoC) has a major influence on DF. As we all know its function is to record any conceivable detail of digital evidence. We moved the chain of custody over blockchain hyperledger sawtooth. Blockchain is a distributed ledger technology that allows data to be exchanged without the presence of a third party, there is no central authority to supervise transactions, thus they would be sent to all network users, who receive, validate, and verify them in a ledger. To improve the security we have used consensus algorithm and create the smart contracts on go language after this we deploy a blockchain based authentication framework for security and performance evaluation [1]-[8].

1.1 Capture evidence: In the first step data of evidence is acquire at the network in order to manage, control, and captured traffic.

1.2. Examination: Separation of packets that are been captured individually, and the size of forensics data is also significantly decreased. Data from different sources being filtered and obtained from various locations before being combined into a single network for analysis.

1.3. Analysis: After examination analysis of data that is being received from the accumulation process take place by using pre-processing techniques, investigation process begins in this process.

1.4. Report: The network data are summarized in a report after the analysis process is completed. Forensic data is capture in a network. The main contributions of this paper are discussed as follows:

- In this paper, we proposed a blockchain-enabled distributed architecture for digital forensics chain-of-custody.
- Hyperledger sawtooth adopted to design an efficient smart contract for the purpose of automate transactions.
- Distributed ledger preservation is designed using Filecoin,
- and tables should be placed in the middle of a page.

2. BACKGROUND:

As we know blockchain is a technology that has taken the world by storm. It is treated as a big thing since internet. It is a peer-to-peer network because of that distributed ledger maintain their consistency. After that, it has an immutable behaviour because of the hash function. Firstly, it was known for its role in cryptocurrency that is very famous it makes it easy to do transactions in real-time by doing that we are able to protect the privacy of the system after that smart contract were developed that are being used till now. Many platforms were implemented but hyperledger was the first one it has various frameworks and all have some features. The Fabric was being developed to creates scalable blockchain applications. Hyperledger burrow seems to be a Linux foundation hyperledger project that enables blockchain clients to create a valid smart contract. Hyperledger Indy is uses to establish a digital identity in a blockchain network it is immune from malicious attacks because it protects the user’s personal information. Aroha is development a mobile application but, we are working on Sawtooth that is quite advance and works as a permission blockchain framework for building a network and distributed applications.

3. PROBLEM STATEMENT

In this era security is the main concern everyone want to keep their information private and protected. Previously a chain of custody was based on a traditional documented from that chould be easily stolen or compromise ,which was then transformed into a digital form using hash values, digital signatures, and encryption techniques. However, there was still some uncertainty about the system that needs to be addressed, There was the possibility that anyone might change the CoC ledger value and hash values, risking the system's integrity, and various privacy problems. Due to above mentioned security concerns, we are moving the chain of custody towards a blockchain hyperledger sawtooth framework that provides efficiency to the chain of Custody and make the system more advance and trustworthy [8]-[15].

4. OBJECTIVE OF STUDY

Following are the main objectives of our project

• Our basic aim is to make the system rigging free by creating a decentralized (Dapp), which removes the threats of such centralized storage.

- The chain of custody will be decisive as a result of our project.

- It will fully secure the entire mechanism of digital forensics CoC
- It will help those who are extremely cautious with manual record keeping.

5. MOTIVATION

We want to rectify the digital forensics of Pakistan so that every victim could obtain justice and feel free. To do so we have received support and motivation from the supervisor he gives us an idea by recommending the use of blockchain technology in DF which is currently the most convincing source for providing security in order to make the system free of manipulation.

6. SIGNIFICANCE AND LIMITATIONS

Since the emphasis of this project is to make the system decentralized that make it secure. It will be exceptionally significant for digital investigators in transforming their systems into a convenient environment. It will increase effectiveness by making it easier to identify data sources correctly early in the investigation process, as a result of this project a highly secure java-based distributes application will be developed. There are also contain restrictions of this project, that are classified as.

- Cost, security, scalability, and efficiency.
- Lack of standardization.
- Improved record transparency
- Regulatory compliances.
- Strengthened Chain of custody processing with digital forensics.

7. PROJECT METHODOLOGY

This paper proposed method that makes blockchain more efficient in order to build trust and transparency. We have use hyperledger in CoC because it is open source and only the parties involved in a specific case can update their ledger. In Hyperledger there is a concept of channels that are essentially virtual blockchain networks with their own access data we have use Sawtooth it is permissioned blockchain framework for building a network and distributed applications unlike many popular blockchains. It also has an advanced scheduler and hot-Swapping consensus algorithm, which ensures that the smart contracts are safe. Without needing to understand the underlying architecture of the system application can define their own rules.

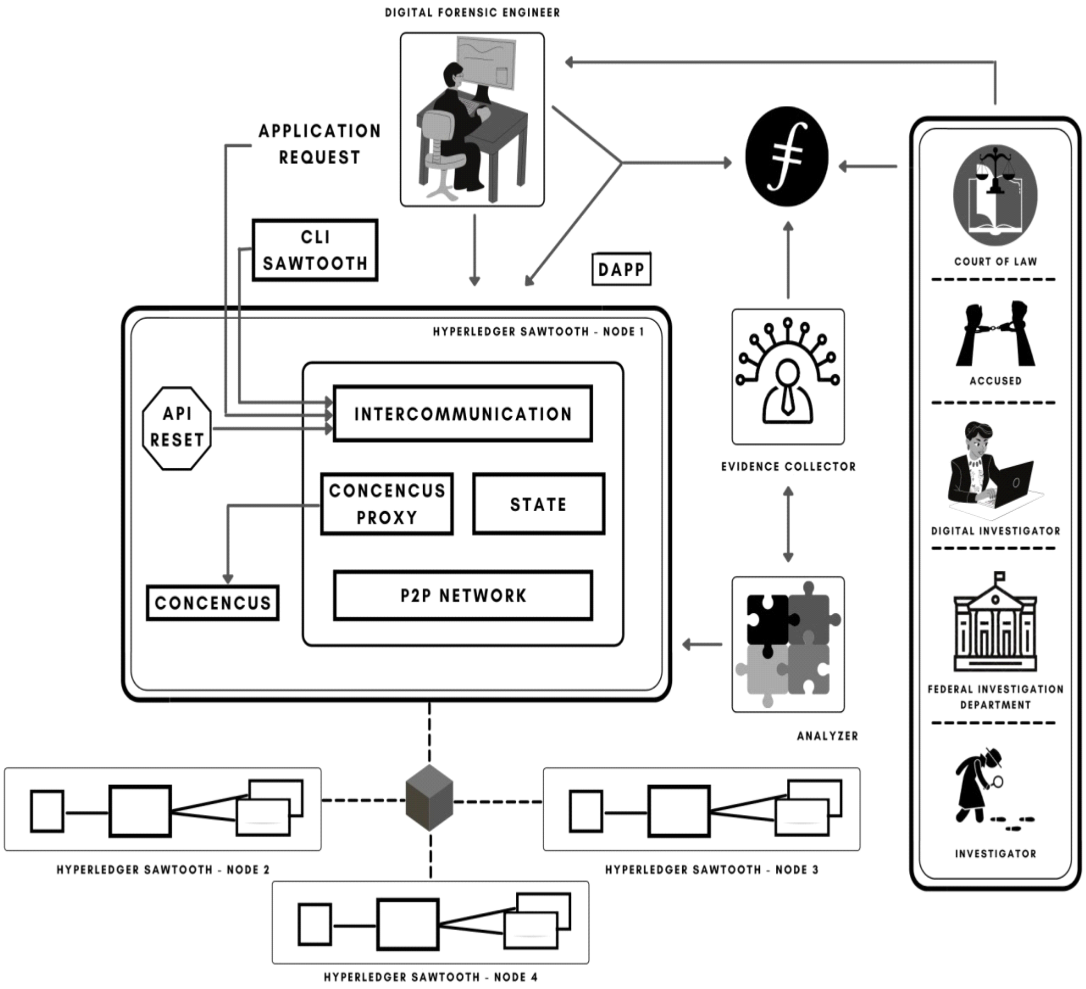
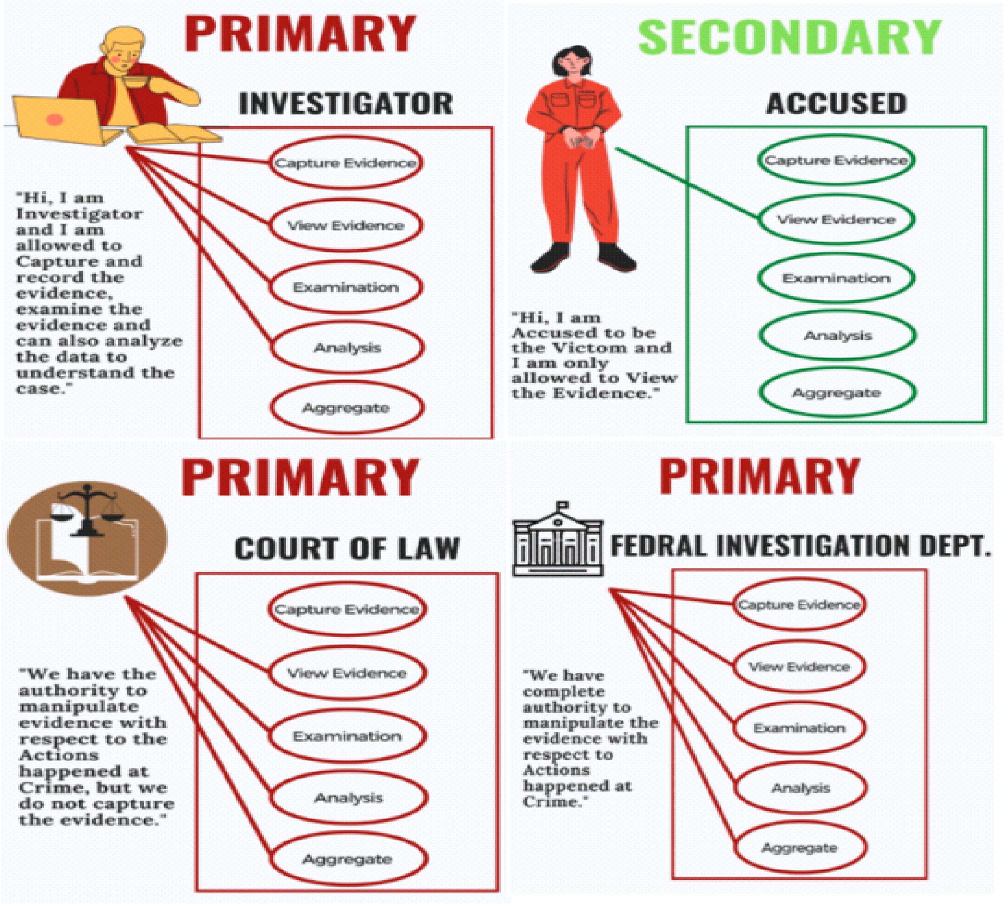


Figure 1: Process Model of Blockchain using Hyperledger Sawtooth

In this model the evidence is captured in the network, examination process makes the evidence available to the system and transfer it for analysis process, the analysis applies pre-processing techniques for investigation, and eventually the whole process is recorded in a report. We have given a concept of digital forensic engineer that has full control on all the stakeholders i.e., accuse, the court of law, victim, and investigator every stakeholder is restricted to take his permission before doing any changes in a ledger [16]-[25]. There are so many ledgers in an architecture Digital forensics engineer can check and trace every ledger with the help of distributed application, a sawtooth node simply contains Sawtooth CLIs that has numbers of commands, Consensus that provide language independency, State sawtooth shows the status of nodes either it is connected or not, reset API's has important role it is use for fetching of object related to the case.

8. USE CASE

This use case disgram defines the roles of each user involed in our system. The job of Investors' is to capture the record of evidence than examine the evidence he can also analyse the data to understand the cases but he is not able to aggregate the evidence. Accused is authorized to view the evidence he cannot examine, analysis, and aggregate of the evidence after, that court of law has the authority to manipulate evidence with respect to the action or crime. He can view, examine, analyse, aggregate the evidence but cannot capture evidence. The Federal investigation department have full authority of the system.



"Hi, I am Investigator and I am allowed to Capture and record the evidence, examine the evidence and can also analyze the data to understand the case."

"Hi, I am Accused to be the Victom and I am only allowed to View the Evidence."

"We have the authority to manipulate evidence with respect to the Actions happened at Crime, but we do not capture the evidence."

"We have complete authority to manipulate the evidence with respect to Actions happened at Crime."

Figure 2: Use case diagrams of the system

9. CONCLUSION AND FUTURE WORK

People mistakenly believe that blockchain is all about cryptocurrency and bitcoins. In this project, we have concluded the need and use of blockchain as we know all the transactions on a blockchain are unalterable, indicating they can't be edited or modified by anyone, we'll be integrating CoC to a blockchain where all transactions related to evidence, accuse, victim, and investigators will be digitally collected through a fixed structure and every block will be protected using hash encryption. In digital forensics CoC, we have used Hyperledger sawtooth platform in the investigation process which is well known to provide security during transactions, in order to makes the system protected and secure it has advanced consensus algorithms which would be beneficial into keeping the system safe and stable, in this project, we have used hash-based encryption acquired by SHA-256, which would be widely expected to provide security and protection to digital forensics and chain of custody, as we know blockchain technology is rapidly evolving day by day, we will implement SHA-512 in future to make system more reliable and secure.

10. ACKNOWLEDGMENT

We would like to pay sincere appreciation to our BSCS supervisor, **Mr. Abdullah Ayub Khan** (Lecturer, Department of Computer Science and Information Technology), and FYP Coordinator, **Dr. Mazhar Ali Dootio** (Associate

Professor, Chairman Department of Computer Science and Information Technology), at Benazir Bhutto Shaheed University Lyari, Karachi 75660, Pakistan.

They both convincingly guided and encouraged us to be professional and set the right path when the road got tough. Without their continuous guidance and persistent help, this research would not have been completed.

Reference

[1] Meng Li, Chhagan Lal, Mauro Conti, Donghui Hu, LEChain: A blockchain-based lawful evidence management scheme for digital forensics, Future Generation Computer Systems, Volume 115,2021, Pages 406-420, ISSN 0167-739X,

[2] S. Li, T. Qin, and G. Min, "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems," IEEE Trans. Computer. Soc. Syst., vol. 6, no. 6, pp. 1433– 1441, 2019, doi: 10.1109/TCSS.2019.2927431.

[3] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," Digit. Investigation., vol. 28, pp. 44–55, 2019, doi: 10.1016/j.diin.2019.01.002.

[4] Zhihong Tian, Mohan Li, Meikang Qiu, Yanbin Sun, Shen Su, Block-DEF: A secure digital evidence framework using blockchain, Information Sciences, Volume 491, 2019, Pages 151-165, ISSN 0020-0255,

[5] X. Burri, E. Casey, T. Bollé, and D. O. Jaquet-Chiffelle, "Chronological independently verifiable electronic chain of custody ledger using blockchain technology," Forensic Sci. Int. Digit. Investig., vol. 33, no. xxxx, 2020, doi: 10.1016/j.fsidi.2020.300976.

[6] E. Nyaletey, R. M. Parizi, Q. Zhang, and K. K. R. Choo, "BlockIPFS - Blockchain-enabled interplanetary file system for forensic and trusted data traceability," Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019, pp. 18–25, 2019, doi: 10.1109/Blockchain.2019.00012.

[7] V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, and S. Katsikas, "A forensics-bydesign management framework for medical devices based on blockchain," Proc. - 2019 IEEE World Congr. Serv. Serv. 2019, vol. 2642–939X, pp. 35–40, 2019, doi: 10.1109/SERVICES.2019.00021.

[8] A. J. Ehrenberg and J. L. King, "Blockchain in Context," Inf. Syst. Front., vol. 22, no. 1, pp. 29– 35, 2020, doi: 10.1007/s10796-019-09946-6.

[9] D. O. Jaquet-Chiffelle, E. Casey, and J. Bourquenoud, "Tamperproof timestamped provenance ledger using blockchain technology," Forensic Sci. Int. Digit. Investig., vol. 33, no. xxxx, p. 300977, 2020, doi: 10.1016/j.fsidi.2020.300977.

[10] D. Billard, "Tainted Digital Evidence and Privacy Protection in Blockchain-Based Systems," 27 Forensic Sci. Int. Digit. Investig., vol. 32, p. 300911, 2020, doi: 10.1016/j.fsidi.2020.300911.

[11] A. Tanner and J. Bruno, "Timely: A Chain of Custody Data Visualizer," Conf. Proc. - IEEE SOUTHEASTCON, vol. 2019-April, pp. 1–5, 2019, doi: 10.1109/SoutheastCon42311.2019.9020497.

[12] P. C. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," Futur. Gener. Comput. Syst., vol. 102, pp. 902–911, 2020, doi: 10.1016/j.future.2019.09.028.

[13] R. Montasari and R. Hill, "Next-Generation Digital Forensics: Challenges and Future Paradigms," Proc. 12th Int. Conf. Glob. Secur. Saf. Sustain. ICGS3 2019, pp. 205–212, 2019, doi: 10.1109/ICGS3.2019.8688020.

[14] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, “Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment,” IEEE Internet Things J., vol. 8, no. 4, pp. 2116–2123, 2021, doi: 10.1109/JIOT.2020.3037733.

[15] Y. L. Gao, X. B. Chen, G. Xu, W. Liu, M. X. Dong, and X. Liu, “A new blockchain-based personal privacy protection scheme,” Multimed. Tools Appl., 2020, doi: 10.1007/s11042-020-09867-6

[16] Khan, Abdullah Ayub, and Syed Asif Ali. "Network forensics investigation: behaviour analysis of distinct operating systems to detect and identify the host in IPv6 network." International Journal of Electronic Security and Digital Forensics 13, no. 6 (2021): 600-611.

[17] Laghari, A.A., Wu, K., Laghari, R.A. et al. A Review and State of Art of Internet of Things (IoT). Arch Computat Methods Eng (2021). https://doi.org/10.1007/s11831-021-09622-6 May 2020, vol. 1501, no. 1. doi: 10.1088/1742-6596/1501/1/012022.

[18] Khan, Abdullah Ayub, Asif Ali Laghari, and Shafique Ahmed Awan. "Machine learning in computer vision: A review." EAI Transactions on Scalable Information Systems (2021): e4.

[19] Ayub Khan, A., Laghari, A. A., Shaikh, A. A., Bourouis, S., Mamlouk, A. M., & Alshazly, H. (2021). Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission. Applied Sciences, 11(22), 10917.

[20] Khan, Abdullah Ayub, Zaffar Ahmed Shaikh, Larisa Belinskaja, Laura Baitenova, Yulia Vlasova, Zhanneta Gerzelieva, Asif Ali Laghari, Abdul Ahad Abro, and Sergey Barykin. "A Blockchain and Metaheuristic-Enabled Distributed Architecture for Smart Agricultural Analysis and Ledger Preservation Solution: A Collaborative Approach." Applied Sciences 12, no. 3 (2022): 1487.

[21] Shaikh, Zaffar Ahmed, Abdullah Ayub Khan, Laura Baitenova, Gulmira Zambinova, Natalia Yegina, Natalia Ivolgina, Asif Ali Laghari, and Sergey Evgenievich Barykin. "Blockchain Hyperledger with Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture." Applied Sciences 12, no. 5 (2022): 2534.

[22] Khan, Abdullah Ayub, Asif Ali Laghari, De-Sheng Liu, Aftab Ahmed Shaikh, Dan-An Ma, Chao-Yang Wang, and Asif Ali Wagan. "EPS-Ledger: Blockchain Hyperledger Sawtooth-Enabled Distributed Power Systems Chain of Operation and Control Node Privacy and Security." Electronics 10, no. 19 (2021): 2395.

[23] Khan, Abdullah Ayub, Asif Ali Laghari, Aftab Ahmed Shaikh, Zaffar Ahmed Shaikh, and Awais Khan Jumani. "Innovation in Multimedia Using IoT Systems." Multimedia Computing Systems and Virtual Reality: 171-187.

[24] Khan, A. A., Shaikh, Z. A., Baitenova, L., Mutaliyeva, L., Moiseev, N., Mikhaylov, A., ... & Alshazly, H. (2021). QoS-Ledger: Smart Contracts and Metaheuristic for Secure Quality-of-Service and Cost-Efficient Scheduling of Medical-Data Processing. Electronics, 10(24), 3083.

[25] Khan, Abdullah Ayub, Aftab Ahmed Shaikh, Zaffar Ahmed Shaikh, Asif Ali Laghari, and Shahid Karim. "IPM-Model: AI and metaheuristic-enabled face recognition using image partial matching for multimedia forensics investigation with genetic algorithm." Multimedia Tools and Applications (2022): 1-17.