This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

MF-Ledger: Blockchain Hyperledger Sawtooth-enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture

Abdullah Ayub Khan[1,3], Mueen Uddin[2], Aftab Shaikh[1], Asif Ali Laghari[1], Adil Rajput[4]

[1] Department of Computer Science, Sindh Madressatul Islam University, Karachi, Sindh, Pakistan
[2] Digital Science, Faculty of Science, Universiti Brunei Darussalam, Jln Tungku Link, Gadong, BE1410, Brunei Darussalam
[3] Department of Computing Science and Information Technology, Benazir Bhutto Shaheed University Lyari, Karachi, Sindh, Pakistan
[4] Department of Computer Science, College of Engineering, Effat University, Jeddah, 21478, Saudi Arabia

Corresponding author: Abdullah Ayub Khan (e-mail: abdullah.khan00763@gmail.com).

ABSTRACT Due to globalization and worldwide connectivity, multimedia data exchange has increased significantly over the Internet in the last decade. The life cycle of multimedia content is also getting more multifaceted as more people are accessing, sharing, modifying and re-using multimedia information. This poses serious challenges for the multimedia industry to provide integrity, reliability and trustworthiness for multimedia investigations against the growing cybersecurity threats. This paper bridges this gap by enabling a secure and transparent digital forensic investigations process using blockchain technology. MF-Ledger a Blockchain Hyperledger sawtooth-enabled novel, secure and efficient digital forensic investigation architecture is proposed where participating stakeholders create a private network to exchange and agree on different investigation activities before being stored on the blockchain ledger. We have created digital contracts (smart contracts) and implemented them using sequence diagrams to handle the stakeholders' secure interaction in the investigation process. The proposed architectural solution delivers robust information integrity, prevention, and preservation mechanism to permanently and immutably store the evidence (chain of custody) in a private permissioned encrypted blockchain ledger.

INDEX TERMS Blockchain; Hyperledger Sawtooth; Smart Contracts; Digital Signatures; Digital Forensics; Evidence Chain of Custody.

I. INTRODUCTION

The handling of gigantic and enormous amounts of data business enterprises use has emerged as one of the challenging tasks in today's IT business world [1]. The increased adoption of social media and other e-business platforms are posing serious challenges and paving the way for digital crimes called cybercrimes. The increased use of various types of heterogeneous data including images, audios, videos and textual data are contributing immensely towards rising trends of cybercrimes in the business world. Digital forensics is being continuously used that involves techniques and practices to investigate, analyze and handle the radical impact of these cybercrimes. The use of social networking and business applications on handheld mobile devices, laptops, tablets and other gadgets in public networks implies that a large amount of personal and business data is always subject to information theft, leakage and other privacy concerns. These crimes have grave consequences for business enterprises and they require secure and transparent digital crime investigation techniques and processes to investigate various types of cybercrimes involving robust detection controls [2].

In today's ever-growing digital world where we are facing huge challenges in securing our digital infrastructures against different types of cybersecurity incidents. Digital forensics plays an important role and becomes of utmost importance to investigate such incidents to find out the actual impact of these crimes as well as how to stop such incidents. With every passing day, digital forensics is attaining more and more acceptance and admiration as it is being used to collect, store, analyze and prove facts to convict intruders involve in these crimes. These investigations lead to the acquisition, analysis, detailed evaluation and interpretation of the collected evidence related to the incident. The findings from the analysis help to further interpret and attribute the incident and can be documented and presented in the form of expert forensic

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

reports, depositions and testimonies to be admissible in a court of law [3].

Furthermore, these digital forensic investigations must ensure validity, authenticity and reliability of the collected evidence against cybercrimes to make sure that the collected evidence is well preserved, secured in a proper container and stored at a locked and reliable place so that it can't be tampered with [4]. It is, therefore, enormously important to realize the transparency and secrecy of the whole digital forensic investigation process life cycle. Digital evidence will be considered acceptable and admissible in the court of law if its original, authentic, comprehensive, steadfast and trustworthy, along with transparent, explainable and with a complete chain of evidence [4]. There is, however, a lack of standardized procedures and mechanisms in traditional digital forensic investigations making them inherently vulnerable to various tampering and forgery occurrences. Such incidents typically occur due to the continuous technological advancements and lack of knowledge and expertise at the forensic expert level when they are collecting, storing and analyzing the forensic evidence for a particular cybercrime use case [5].

In the multimedia forensics domain, similar vulnerabilities and limitations are worth mentioning. Some of these incidents include differentiation and identification between original and copy-move forgery events and shreds of evidence critical for the record-keeping purpose for every event that happened while investigating a specific cybercrime. These attributes pose significant information integrity and preservation challenges [6]. Another challenge is the complexity of hiding innumerable types of digital information in a carrier signal over multimedia systems causing the carrier's channel's to prove their authenticity and validity during a cyber incident [7]. Furthermore, the remote evidence acquisition process itself is highly vulnerable while collecting digital evidence from different sources on the network including handling data nodes from an entry point of discovery to evidence remote data recovery, reconstruction, and verification [8, 9]. This traditional layered process is considered insecure, while collecting, preserving, and storing the digital evidence [10]. The database systems involved also can't maintain and preserve the integrity, originality and confidentiality of the collected evidence as well as the related chain of custody of various events that occurred in a specific sequence while collecting, transferring, storing, analyzing and interpreting the evidence to solve a cybercrime incident [11, 12]. While on the other hand cybercriminals instigate malicious activities through multimedia and network devices such as business credential leakages, information theft and unauthorized access [13]. This allows hackers and other intruders to forge and tamper with the collected evidence. In summary, we have identified five (5) critical challenges and problems in multimedia forensics and are classified as follows:

1. Media forgery and digital watermarking
2. Editing tools for manipulating investigational technical contents
3. Remote evidence acquisition, chain of custody, and reconstruction vulnerabilities
4. Botnet attacks
5. Live media evidence collection challenges

The multimedia digital forensic investigation process comprises of five (5) layers [15]. The process includes data acquisition from the media device, performing forensic analysis of the crucial aspects of the collected data to extract the meaningful evidence and submitting a comprehensive report for further evaluation and interpretation for the case under investigation in a court of law as shown in figure 1. The collected evidence and related chain of custody events must be preserved and protected for further investigations.

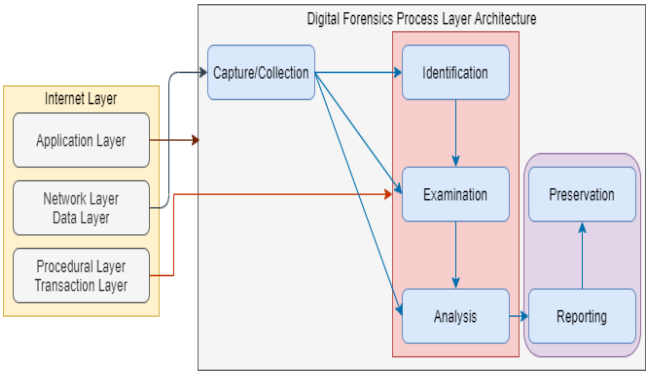

FIGURE 1. Traditional layered digital forensics investigational process

The existing digital forensic investigation process while solving cybercrime is explained below with different processes involved to comprehend the whole process. These processes are:

1. Collection: It involves collecting the relevant and seized digital electronic multimedia contents that are relevant to the case under investigation from different multimedia devices. The process encompasses different methods such as imaging, copying, and reorganizing the collected digital evidence and storing it in a secure and protected container.
2. Identification: Finding out the potential sources of most significant and valuable information and its ownership and location of data.
3. Examination and Analysis: Detailed systematic examination and searching of correlated information are being investigated related to the crime. The data objects retrieved include device information, network paths, user-generated logs and cookies and other relevant details. Further analyses were performed to reach some meaningful

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

conclusions based on the evidence collected and examined.

4. Reporting: In this phase, a complete report is generated based on the evidence examined and analyzed using appropriate forensic techniques. The report is then submitted in the court of law as complete evidence against the case under investigation.
5. Preservation: Electronically preserve the collected evidence by protecting the multimedia devices, capturing device-related records and user logs, and documentation of all the relevant evidence securely.

Blockchain technology is currently enabling enterprises to secure their existing systems and processes specifically supply chain systems to realize privacy, transparency, provenance, traceability, and easier access to information through DApp and access APIs in almost all aspects of computing information systems. In digital forensics blockchain can also help secure, encrypt, and store the evidence and case transactions on an immutable ledger to enable a transparent multimedia forensics investigation process [14]. Further, the chain of custody transactions and events can be stored in a chain structure in a gazette order connected through various channels in a private permissioned Hyperledger network. Furthermore, the business logic is managed and controlled through smart contracts called smart contracts to achieve the decentralized autonomous investigation application in digital forensic investigations. This helps to achieve secure, transparent and immutable multimedia digital investigations which are hard to forge and temper with, along with encrypted evidence preservation and storage in a secure storage container [16].
Blockchain has already been envisioned and used by various industrial supply chain systems to achieve transparency, provenance and traceability to enable evidence preservation and analysis [17, 18]. Many forensics experts are using blockchain as its decentralized and distributed architecture protects against a variety of malicious attacks usually intended for centralized systems and architectures. This enables to enhance the decentralized node defense ability by using cryptography and hashing functions along with the deployment of intrusion detection and prevention systems, installation of firewalls, anti-disclosure tools and policies to guarantee the immutability, transparency, and distributed trust within the case under investigation [19].

A. MOTIVATION

In this paper, a novel and secure Hyperledger Sawtooth-enabled blockchain architecture for Multimedia digital forensic investigations is proposed. The proposed MF-Ledger architecture provides complete data provenance, traceability, and assurance for performing different operations as well as trust between the chain of custody events while collecting, storing, analyzing, and interpreting the digital evidence. This ensures privacy protection for the whole transactional evidence preserved in distributed blocks of data in an encrypted ledger [20]. The main contributions of this research are as follows:

1. We present a discussion of the problems and limitations of the digital forensics chain of custody process.
2. MF-Ledger a Blockchain-enabled digital forensic investigation architeture is presented.
3. It presents various algorithms for smart contracts (business rules) and their implementations.
4. The proposed architecture is simulated using sequence diagrams in a private permissioned Hyperledger network.
5. Blockchain implementation open challenges are discussed with future research directions.

The rest of the paper is organized as follows. In section 1, we discuss the existing digital forensics investigation process involving chain of custody, blockchain technology. In section 2, we discussed various related research and requirements. In Section 3, we proposed how blockchain can be useful to secure, protect and attain chain of custody. In section 4, we proposed the blockchain-enabled chain of custody architecture and its working. In section 5, we presented algorithms for various smart contracts and sequence diagrams. In section 6, blockchain implementation challenges are presented. Finally, we conclude the paper in Section 7.

II. RELATED WORK

This section will review and highlight the related work done on securing the digital forensic investigation process. The authors in [21-22] presented benefits of digital forensics that offer multimedia investigation but did not highlight the solution for preserving evidence in an ongoing case involving events in a chain of custody and sharing information through the multimedia-based portable device on the cloud environment. Nyaletey et al. presented a BlockIPFS approach that concerns the clear audit trail and tackles underpinning security issues, especially access control, especially lack of file traceability and secure preservation [23]. Jeong et al. presented a solution for designing and implementing a blockchain Hyperledger fabric enabled permissioned forensics investigational model to improve trustworthiness authorship in the cyber environment. This architecture doesn't provide a mechanism that allows authorized stakeholders to share and manage potential case information in a distributed ledger environment [24]. Moreover, table 1 highlights and discusses several similar blockchain-enabled approaches that focus on different solutions comprising collaboration of blockchain-enabled decentralized technology and digital forensics techniques.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

TABLE 1: RELATED WORK ON BLOCKCHAIN-ENABLED FORENSICS AND DIGITAL MULTIMEDIA INVESTIGATION

NO	Research Title	Proposed Work	Drawbacks	Reference
1	Forensic chain: Blockchain-based digital forensics chain of custody with PoC in Hyperledger Composer	This research proposed a digital forensics chain architecture, a blockchain-based forensics evidence chain of custody.	1. A comprehensive view of transactions. 2. No promising evidence preservation security. 3. Less evidence integrity and resist forgery. 4. Cross-borders jurisdiction law issues. 5. Fact latency, fragility, and volatility.	[12]
02	Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger	This paper discussed the blockchain-enabled digital forensics and incident response system. Evidence is sustained in the distributed ledger and maintains chronologically ordered documentation, which will present in the legal court.	1. Forensics readiness to the computer systems. 2. Lack of data control. 3. Required an online chain of custody.	[25]
03	Forensic chain: Ethereum blockchain-based digital forensics chain of custody	The paper presents the Ethereum permissionless hyperledger architecture that enables a digital forensics chain of custody.	1. No guaranteed digital evidence integrity, authenticity, auditing platform. 2. Not support a real-time cybercrime evidence process layer 3. Permissionless blockchain.	[26]
04	A blockchain-based chain of custody for evidence management in digital forensics	Proposed blockchain-based chain of custody (B-CoC) architecture that aims to guaranteed audit integrity of digital evidence collection and stakeholder traceability.	1. No direct modification or alteration without permission. 2. Cannot handle multiple stakeholders. 3. No proper management of evidence.	[27]
05	LEChain: A blockchain-based lawful evidence management scheme for digital forensics	The work presents LEChain, a blockchain-enabled evidence management model, which supervises evidence collection flow, court votes, and trail-based results.	1. This study has adopted cloud computing existing evidence. 2. Not fully support information transparency and auditing. 3. The scheme only covers weak security. 4. It can't cover the entire life cycle of the evidence process layer. 5. Does not address forensics privacy issues.	[28]
6	A blockchain-based Forensic Model for	This paper demonstrates the embezzlement method designed for digital forensics	1. Blockchain-based method adaptability.	[29]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

	Financial Crime Investigation: The Embezzlement Scenario	investigation. The proposed framework functionally implements blockchain smart contract and integrates standardized forensics evidence collection flow and chain of custody evidence preservation tools and techniques.	2. Addresses financial crime significantly impacts financial services. 3. A symbiotic relationship between financial digital investigation and blockchain technology with a lot of challenges.	
7	Digital Forensics: Maintaining Chain of Custody Using Blockchain	The proposed work discussed the secure blockchain-based digital evidence collection, examine, analyzed, and investigate the cyberthreat, in short, maintain immutable evidence along with the integrity of the decentralized chain of custody application for preserve the distributed lawfully case information and present this in the legal court.	1. Authentic and remains original evidence without forged. 2. Not fully recording and preserve digital crime incidents. 3. Handle individual criminal activities.	[30]

After critically reviewing the related literature, we identified gaps in the previous work and proposed our solution based on blockchain hyperledger sawtooth, a permissioned based distributed ledger architecture that aims to provide secure evidence integrity, preservation, transparency, and resist temptation. The proposed solution covers the entire life cycle of evidence collection to the preservation and handles various stakeholders at the same time. We also provide a secure and authentic decentralized network platform that manages the evidence chain of custody and guaranteed secure protection chain of custody evidence in a gazette encrypted digital ledger.

III. BLOCKCHAIN SECURITY IN DIGITAL FORENSICS

Digital Forensic investigation is a systematic and methodological process for the identification, preservation, collection, analysis and presentation of digital evidence to be admissible in a court of law. To accomplish that, maintaining chain of custody is a critical prerequisite and must be established throughout the digital investigation process. Chain of custody (CoC) is a process of recording, documenting and preserving the chronological order and complete history of handling and maintaining the digital evidence for the case under investigation to be admissible in a court of law. It is certainly imperative to keep CoC protected from being transformed or demolished. The ultimate goal is to prove that collected evidence is true, factual and relevant to the crime under investigation.

Blockchain has been widely adopted and used in a wide range of security applications to provide immutable distributed ledger solutions for storing and protecting blocks of data in a chain structure. This enables storing hashed encrypted data with digital signatures so that it cannot be altered by others without the permission of participating stakeholders on the permissioned blockchain network [2]. This immutable ledger technology proposed in the blockchain architecture aids additional controls to handle and maintain the digital evidence securely and transparently throughout the forensic investigation process. There are three main characteristics of blockchain as follows:

1. This technology is open to every participating stakeholder who joins the blockchain network and participates to access the transactions on the ledger. The users can access the blockchain network through an open application interface.
2. Blockchain uses a decentralized and distributed P2P network communication model in which all participating stakeholders can equally participate and access the network thus eliminating the requirement for a third-party platform and solution providers.
3. Each block carries an encrypted hash value from the hash of a previously stored block in a secure chain of blocks, making an immutable ledger for storing and preserving the confidential information (evidence) related to the case under investigation. Any amendment in the ledger needs to be agreed, signed, and approved by all participating stakeholders using some consensus algorithms. This is achieved using smart contracts (smart contracts) where all the business logic is designed and implemented. Finally, the verified and agreed blocks of data are stored in the chain in the ledger.

A. CLASSIFICATION AND FEATURES OF HYPERLEDGER TECHNOLOGY

Hyperledger is an open-source blockchain architecture available to the community for developing secure and decentralized DApps for enabling provenance and transparency in different supply chain applications in business enterprises. The hyperledger platform provides various tools

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

like hyperledger composer, hyperledger caliper and other libraries such as Ursa to deploy and implement blockchain at the enterprise level. The hyperledger technology offers multiple platforms to build different blockchain-enabled solutions as given in table 2 below.

TABLE 2: LIST OF DISTINCT HYPERLEDGER FEATURES WITH THEIR DESCRIPTION

Hyperledger	Features	Description
Hyperledger Fabric [31]	1. Modular architecture 2. Plug and play services 3. Consensus enabled performance at scale 4. Preserving privacy 5. Distributed ledger solution 6. Permissioned based 7. Private network	Hyperledger Fabric is a modular architecture-based distributed ledger solution; delivers higher-ordered integrity, availability, confidentiality, flexibility, scalability, and resilience. This architecture design supports to plug distinct components implementation and accommodate complexity that occurs in the existing ecosystem. The hyperledger fabric model promises comprehensive functionality, customized smart contracts, and enterprise blockchain security solutions; some of the crucial factors are Assets, Ledger Feature, Consensus, Chaincode, Privacy and Security Services
Hyperledger Indy [32]	1. Interoperability 2. Distributed ledger 3. Shared components 4. Provide libraries and client tools 5. Decentralised identifier 6. Correlation-resistant 7. Permissionless	The hyperledger Indy is another framework of blockchain distributed ledger that provides libraries, client tools, and components (that can be reusable) for identities. It provides interoperability of the digitally rooted characters on the blockchain that can utilize as powered the identity in a decentralized domain or sometimes standalone.
Hyperledger Besu [33]	1. Open-source 2. Develop Ethereum client 3. Enterprise Ethereum Alliance 4. User facing APIs 5. Performance monitoring 6. IBFT and Clique consensus algorithm 7. Public and private network permissioned or permissionless	Hyperledger Besu is an open-source Java-based Ethereum Client blockchain framework that develops under the license of Apache 2.0. It runs on the Ethereum private, public, and test networks. This framework includes a command-line interface (CLI) and JSON-enabled API; for maintain, run, monitor, verify, validate, debug transactional nodes in the network. The main Besu functionalities are as follows: • Development of Smart Contract • Provide a platform for the development of decentralized applications • Mining Ethers
Hyperledger Grid [34]	1. Framework for building supply chain solution 2. Provide modular components 3. Client interface 4. Domain-specific data model 5. Smart contract	This hyperledger is an open-source project on GitHub, a framework intended to provide reference building of supply-chain-centric data type (includes distributed ledger components), data models, libraries, SDK, business logic-based smart contracts, client interfaces, such as domain-specific application. Moreover, it combines modular components from a stack into a single; this could seem like a practical business solution.
Hyperledger Iroha [35]	1. Role-based access model	Hyperledger Iroha is a permissioned blockchain design simple to incorporate technology like distributed ledger, mainly used for IoT infrastructure developmental projects. The framework has basic

	2. Assets and identity management 3. General-purpose 4. Private network 5. Simple deployment 6. Command query separation	construction features, such as modular, client application development, domain-driven, a fault-tolerant algorithm for consensus secure connectivity. The application is used for private transactional services, such as intrabank settlement, payment systems, central bank financial logs, digital currencies, logistics, and many more.
Hyperledger Sawtooth [36, 37]	1. Distributed ledger applications and networks 2. Safe smart contract 3. Enterprise and consortia make a policy decision 4. A private network, fully permissioned based 5. Parallel transactional execution 6. Pluggable consensus algorithm	The hyperledger sawtooth offers modular architecture and more flexibility that separates the core system from the application domain. Because of the features of the hyperledger, without needing to know the core systems underlying design, we can specify the smart contract according to the transactional business rules. In this regard, the perfect enterprise solution, building, deploying, and running distributed ledgers, such as permissioned transactions, privatize communication, and secure nodes connection.

B. BLOCKCHAIN HYPERLEDGER SAWTOOTH IN MULTIMEDIA FORENSICS

Hyperledger sawtooth is a private permissioned blockchain platform to create enterprise-enabled blockchain solutions to support and build private networks in an immutable distributed ledger [36]. Hyperledger Sawtooth rationalizes blockchain applications by isolating the core system from the application domain, where the sawtooth applications specify the appropriate business rules. Furthermore, it allows choosing a language for business transactions without requiring the internal details of the core system's underlying design. The high modularity further allows sawtooth to enable consortia and enterprises to make the best policy equipping them with better decision-making abilities [37]. The design grants the blockchain application to customize transactional rules and allows the implementation of permissioned and consensus algorithms. A complete hyperledger sawtooth platform includes many properties and characteristics such as consensus algorithms, timestamps, business rules, digital signatures, customized smart contracts.

Blockchain-enabled multimedia forensics investigation technology is usually categorized into multiple layers. These include the application layer, transactional layer, consensus layer, incentives layer, network layer, and data layer [38], as shown in Figure 2. Additionally, we applied the blockchain hyperledger sawtooth to the existing multimedia forensic investigation such as collection, identification, examination, analysis, reporting, and preservation delivers a guaranteed solution for the robust incident response of devices examination and evidence items integrity, traceability, provenance, distributed security, and secure record on the chain of decentralized nodes. Also, blockchain enables investigation with information or evidence authentication, immutability, trustworthiness, and tracking and traceability between the forensics process of digital information examination and analysis.

In multimedia investigations, hyperledger sawtooth securely protects to analyzes the multimedia-enabled digital signals to retrieve the probative evidence. This allows investigators to reveal history, validate digital contents' integrity, identify the acquisition devices, report legal case updates, and retrieve the evidence chain of custody. To accomplish this, each node in the chain generates a private key – this specific key is generated by asymmetric encryption. This private key is used to identify, authenticate and digitally sign the transaction. The existing forensic process is amended with a blockchain layer. The working and functionality of the blockchain-enabled process are explained below:

1. Network layer: in this layer, a private permissioned P2P network is designed with designated participating stakeholders. Each node in the network is considered equal allowing other nodes to interact with the peer network nodes in the topology. The network layer must ensure the validity and verification of the transactions performed on the blockchain network by different nodes. The consensus function enables node effectiveness and encapsulates all the participating nodes in the chain. The common consensus algorithms used are Practical Byzantine Fault Tolerance (PBFT) and Proof of Elapsed Time (PoET).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

2. The Transaction layer: this layer allows forensic logic to be integrated and executed using smart contracts in the digital investigation and distributed process. In smart contracts, digital signatures are validated for the collected evidence to make sure that the presented evidence is reliable, factual and trustworthy based on the forensic evidence laws. Additionally, Sawtooth CLI interconnects with all the transactional nodes and sets the sawtooth command line to interact with different blockchain services.
3. The application layer uses stakeholder DApp SDK for submitting the transactional approval, requesting evidence chain of custody, on-chain communications, etc.

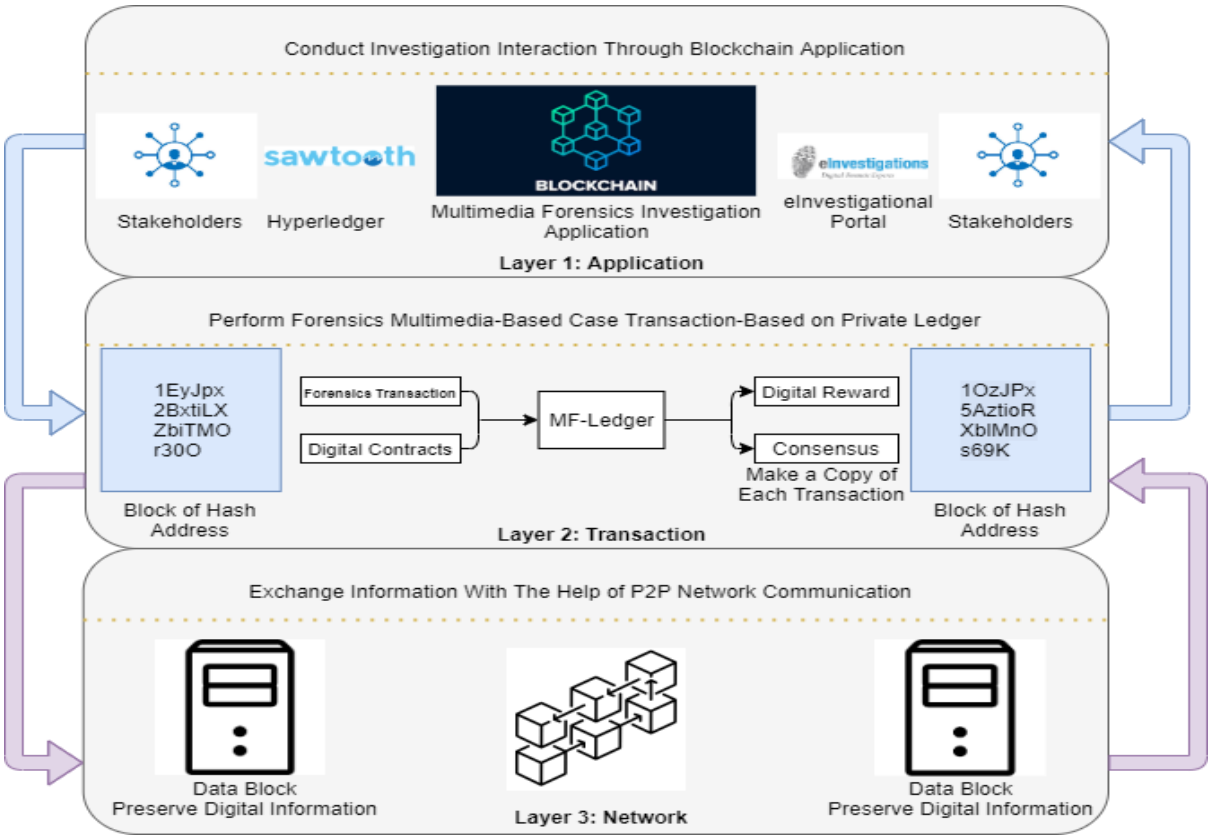

FIGURE 2. **Multimedia forensics investigation using Blockchain Hyperledger Sawtooth**

IV. PROPOSED MF-LEDGER: HYPERLEDGER SAWTOOTH MULTIMEDIA FORENSIC INVESTIGATION ARCHITECTURE

Depending on the magnitude and the case scope, the data capturing and analysis process, evidence integrity, secure data protection and preservation, and evidence chain of custody security are essential challenges. Figure 3 presents MF-Ledger a blockchain hyperledger sawtooth architecture that enables multimedia evidence collection, identification, examination, and reporting of the evidence chain of custody in an investigational context. This proposed architecture demonstrates the complete scenario of the multimedia evidence chain of custody between distributed ledgers security between distinct transactional nodes and maintains consensus proxy for updates the case documentation hash encrypted and evidence preservation. Whereas the stakeholder access blockchain application, such as access the case details, submit transactional approval and apply request for evidence chain of custody through SDK DApp. Digital forensics engineer handles application requests of all the stakeholders. For this purpose, the expert manages logs in the file storage systems and tackling case evidence redundancy challenges. Moreover, the filecoin systems' primary objective is to store case records such as documentation, reporting, timely updates, enclosed mediator, and eventually, the judiciary decision.

Through the proposed blockchain hyperledger sawtooth and forensics architecture, there is an off-chain communication between evidence collector or examiner and multimedia analyzer for the case validation to the present in the judiciary with evidence integrity and preservation. The on-chain communication connects digital evidence collector/examiner and sawtooth transactional node using a smart contract - to ensure the evidence validity, interconnectivity, state for the information status of an active validator and peer to peer network connection between nodes. The node of hyperledger sawtooth case evidence validator has crucial components,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

such as RESET API and the transaction processor. The representational state transfer application programming interface is the internet service development that is used to fetch case objects such as a distributed hypermedia chain of custody system. Furthermore, the transactional processor investigates file records while sawtooth CLI supports a set of commands to interact with hyperledger services. The acyclic interconnectivity between nodes also shares complex sawtooth consensus protocols - implemented as a separate process. The PBFT consensus engine maintains fault tolerance and resolves issues with the original protocol. A PoET consensus simulates an enclave - a trusted execution environment that provides efficient proof of work solution. The proposed blockchain hyperledger sawtooth enables multimedia forensics investigational architecture with robust performance and supports distributed security that helps in ensuring the evidence integrity, confidentiality, and evidence chain of custody protection.

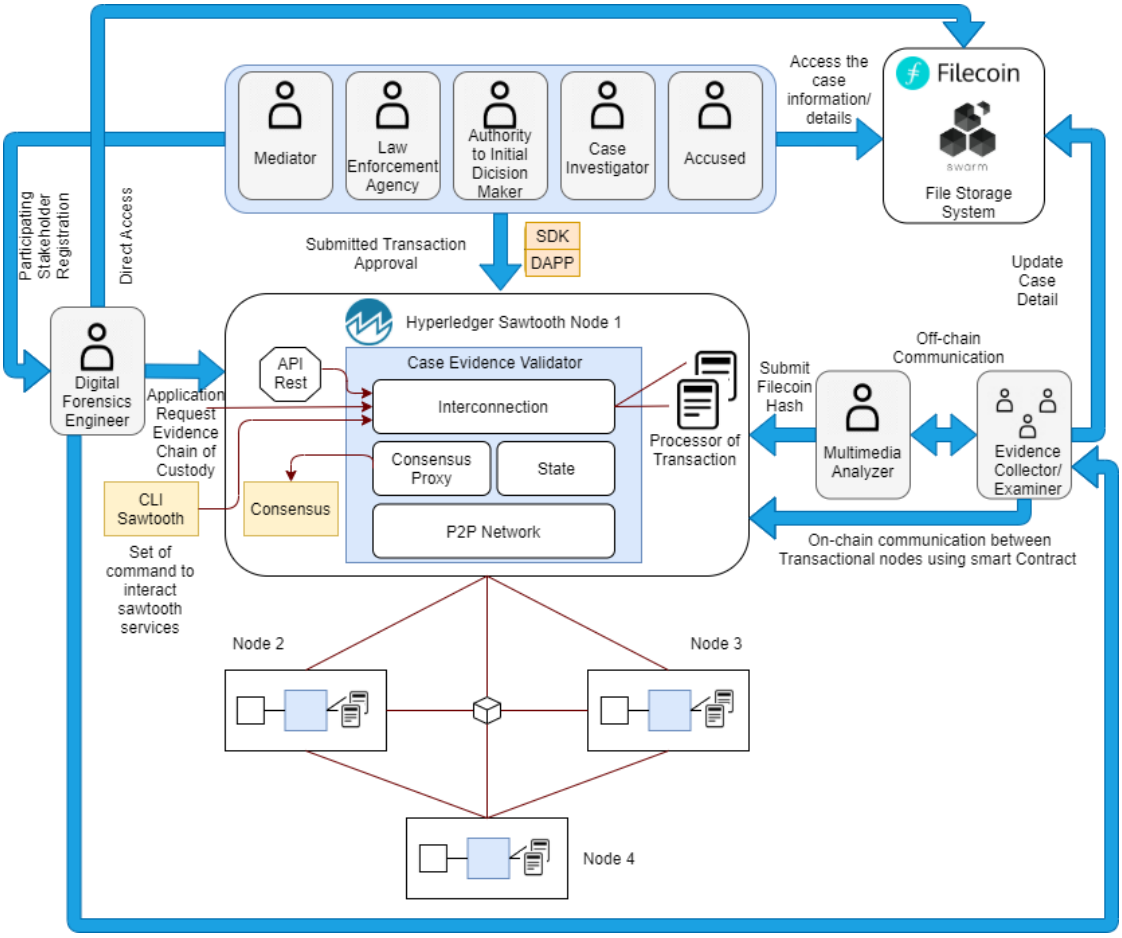

FIGURE 3. **MF-Ledger Hyperledger Sawtooth architecture for multimedia-enabled evidence chain of custody in digital forensics investigation**

A. WORKING OF THE PROPOSED MF-LEDGER ARCHITECTURE

Sawtooth segregates the core digital ledger system from the application that specifies a domain and distributes the ledger of evidence transaction to all the stakeholders in a peer-to-peer network. It is entirely decentralized, and there is no central administrator setup for the evidence chain of custody. The evidence chain of custody distribution is one of the security advantages where case investigation is shared among potentially untrusted stakeholders. Thus, all the nodes in the peer network are demonstrably identical. The nature of sawtooth immutability makes the system robust to detect and prevent alteration attempts while using block hashes. The registered case identities digitally sign all changes performed by forensics transactions. Below we will discuss the mechanism of the proposed sawtooth-enabled investigation architecture.

1) Evidence storage structure

Every transactional data block contains a hash index of the previous block. Any evidential information change in a specific block implies that the other blocks' hash value also changes accordingly, culminating in the reform of the subsequently connected chain of data block hash values. These data structure nodes are composed of a head, and body including the previous hash values of the blocks, version number and a randomly generated number, timestamp, target hash, and Merkle root to verify node data. In summary, the content of the blockchain evidence storage structure is as follows:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

- Sawtooth version 1.2. used to specify the rules of the transaction. Evidence storage reference in the system and record the update of the agreement.
- The evidence structure node has a hash index that forms a chronological order of the chain-like structure shown in figure 4.
- To form a hash root of the transactional node. The individual node calculates hash values according to the Merkle tree.
- The hyperledger sawtooth accumulator averagely divides the workload of PBFT and proof consensus algorithm and starts from the initial stage.
- Intel-based Linux timestamp is used to secure a chain of custody chunks generated for evidence protection and information preservation.
- These consensus algorithms set the targeted critical values of the node iteratively.
- In the end, the node contains transactional information, including input and output addresses, forensics transaction values, and many more.

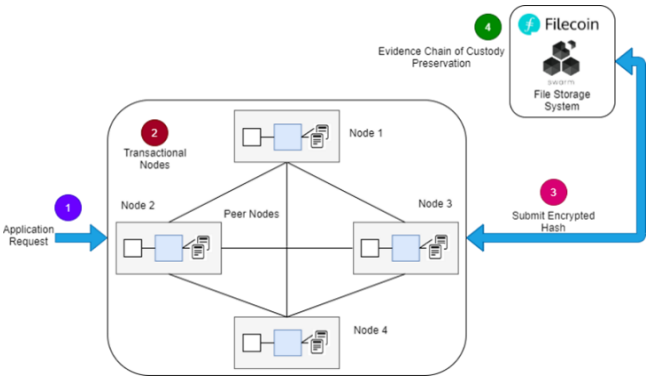

FIGURE 4. Evidence storage structure

2) Network architecture for evidence chain of custody

In this network, the host node of a hyperledger sawtooth evidence chain of custody system runs a single validator, optional REST API, a set of a transaction processor and consensus engine (PBFT) as shown in figure 5. The first transactional genesis block specifies the on-chain setting for the communication network using a customized smart contract; the other nodes access those contractual settings to connect case blocks and join the network. Every transactional node runs the same consensus engine and configures PBFT along with the same set of transaction processors.

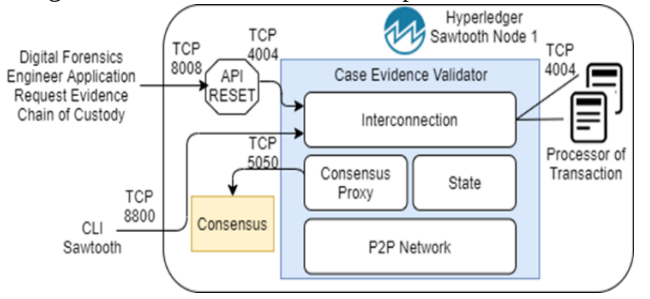

FIGURE 5. Proposed Hyperledger Sawtooth network architecture for evidence chain of custody

However, the routable address in the network configures before starting case evidence validator by digital forensics engineer. The application uses a trust authorization type between all the nodes in the permissioned network, which robust the security between these distributed nodes

3) Sawtooth batch encryption for evidence chain of custody transactions

Due to the private network architecture, the hyperledger sawtooth design for permissioned transactions cannot run as a public network. For this purpose, sawtooth mitigates against distributed denial of service attacks. The communication (zero message queue library) between digital forensics engineer and REST API occurs through TCP port 8008 (TCP's stateful nature also ensures this transaction's integrity). The TCP port 8800 is used to validate case evidence by other stakeholders. Moreover, the transaction processor and RESET API use the TCP ports 4004 and 5050 to utilize the consensus engine on-chain communication shown in figure 6. In the security network, sawtooth flow control rejects frequent transactional submission of stakeholders. The case evidence validator can stop accepting new batches of data nodes' transaction cannot be handled the more investigational task, and case validator can be obtained based on the rollback average that multiplier of the number of batches publication.

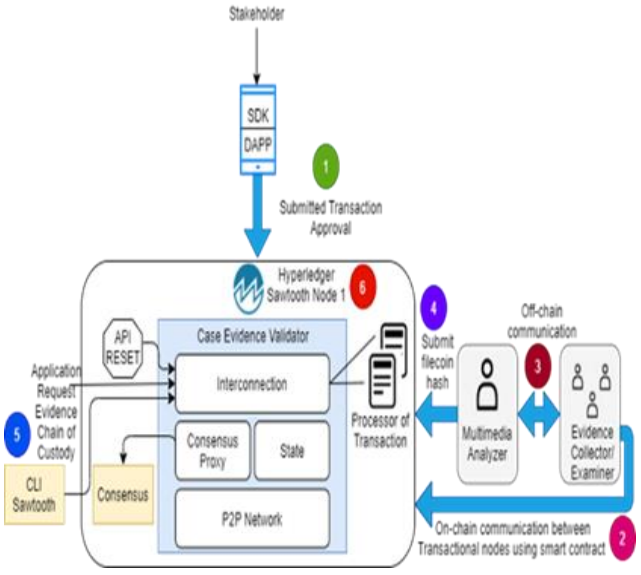

FIGURE 6. Hyperledger Sawtooth Blockchain for case evidence validation

Hyperledger sawtooth receives nodes of all transactions from a stakeholder in the form of a list of batches. This list of batches contains more than one batch and one or more transactions in a single batch that can be processed. The batch encryption with two digital transactions of evidence chain of custody in a single batch is shown in algorithm 2.

4) Digital signature and private chain of custody transaction

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

A non-trivial process of encoding digital evidence information is submitted in a distributed ledger. The SHA-256 standard is used to generate a private key, and the secp256k1 ECDSA standard is used for a digital signature that provides a safeguard to confirm stakeholder identity and data validation. All the transactions are created and serialized with the help of a batch buffer. A hash encrypted with 265 bits of the private key and secp256k1 generates a random set of almost 32 bytes providing a valid key for digital signature. The pseudocode of developing digital signature and submitting private evidence chain of custody transaction is given in algorithm 1 below:

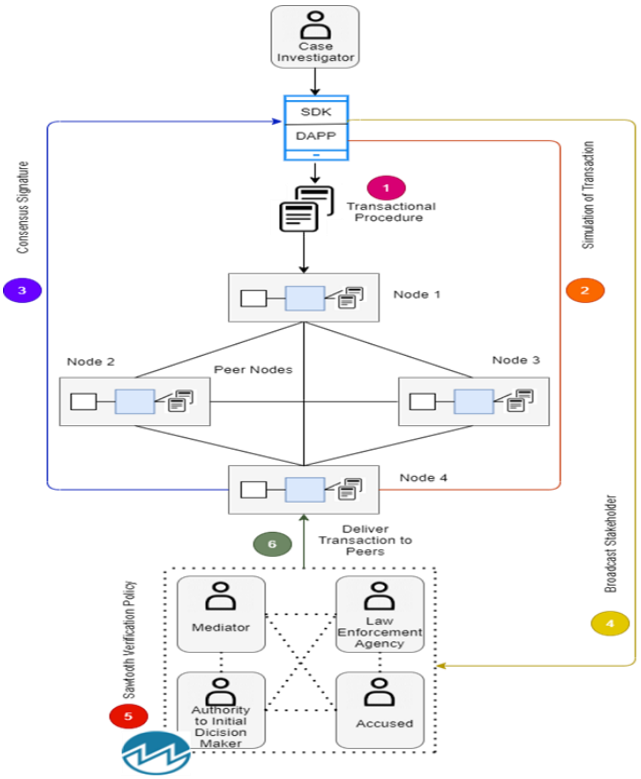

FIGURE 7. Hyperledger Sawtooth privacy mechanism for forensics evidence chain of custody in a blockchain-enabled distributed network

Algorithm 1: Generating digital signature and submitting the transaction

Digital signature and permissioned private transaction:
.head: .head_secp256k1 .key_handle .private_key_byte .public_key_byte_hex .payload_byte .payload_sha256 .transaction_signature .head_signature .payload_sha256_hash_byte .transaction_signature

Algorithm 2: Evidence Chain of Custody Batch Encryption

Batch List:
Batch #1: .head: .sign_private_key#key verification for digital transaction .head_signature
Transaction #1: .head: .sign_private_key .stakholder_batch_private_key .read_state_address .write_state_address .unique_nonce .payload_hash_ sha512_encryption .head_signature .payload_transaction #specific data application
Transaction #2: ….
Batch #2: ….

5) Hyperledger sawtooth enabled privacy of distributed nodes

Hyperledger sawtooth evidence privacy architecture present distributed node transaction architecture where trusted case-related stakeholders submit their application creating a series of forensics transactions with trusted sawtooth hyperledger. A secure case transaction procedure has ensued between nodes when all nodes are connected with a peer network. Changes in any nodes require a consensus digital signature and simultaneously simulate transactional details are transmitted to every stakeholder. After the complete digital signature process, the stakeholders deliver transaction approval to the peers of nodes and is verified by the policy privacy of sawtooth hyperledger.

V. IMPLEMENTATION OF MF-LEDGER HYPERLEDGER SAWTOOTH IN MULTIMEDIA FORENSICS

The implementation of the proposed MF-Ledger architecture is shown using sequence diagrams. Initially, all the stakeholders related to the case under investigation are registered on the distributed blockchain P2P network by a designated forensic authority, which controls and coordinates the whole investigation process. Additionally, new stakeholders can also be added to the network if required after getting verified and digitally signed by the concerned authority. The proposed permissioned network architecture then deploys the SDK application interface to specific investigational clusters of sawtooth nodes with distinct permissions on the same smart contract. Moreover, the ledger preserves the crucial investigational records about the private network, nodes, and stakeholder identities.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

The foremost benefit of using hyperledger sawtooth in the digital forensics process is that it provides robust performance while operating transactional activities on the network as it permits a parallel transaction execution mechanism. Figure 8 presents the complete investigation process that enhances the efficacy and proficiency of the whole forensic investigation process. The other advantage is that the hyperledger sawtooth network architecture allows for better maintenance and security of the chain of custody events during the investigation process.

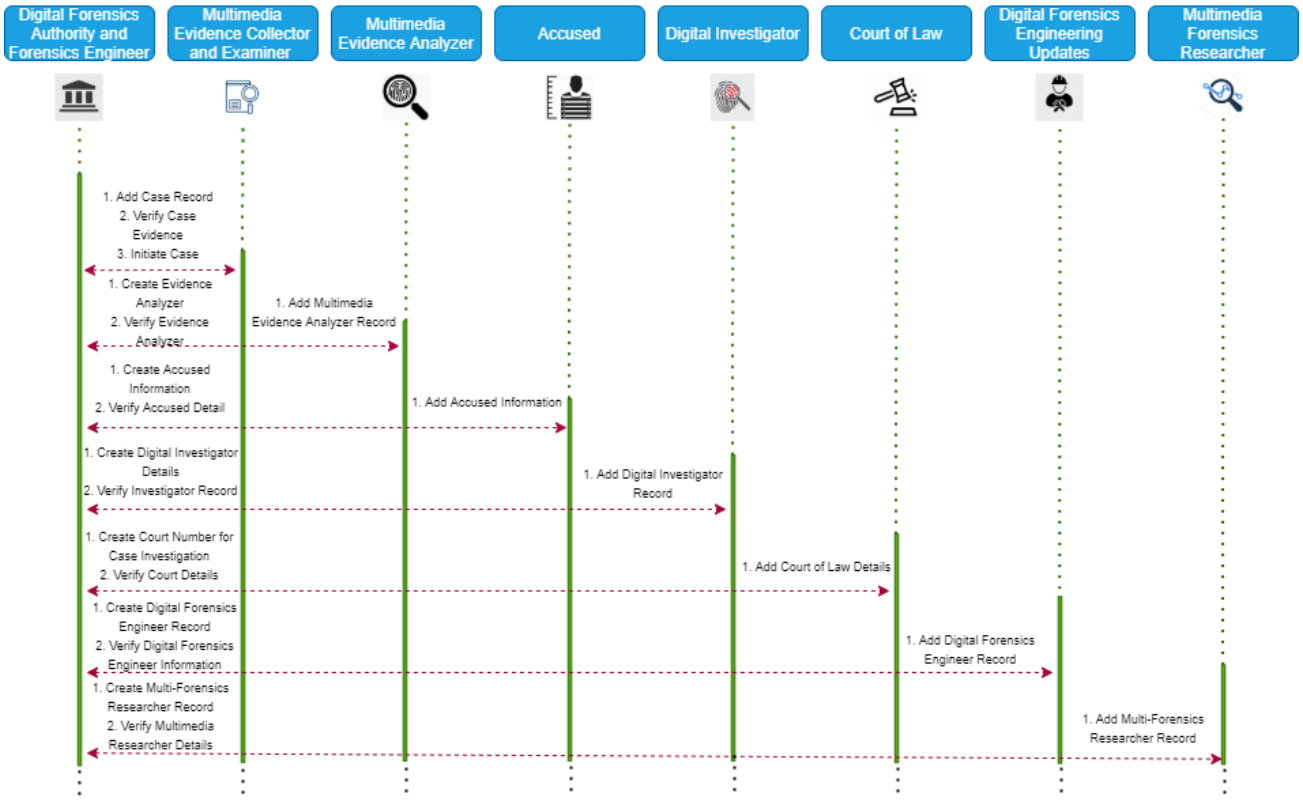

FIGURE 8. Sequence diagram of Sawtooth SDK application implementation for multimedia forensics chain of custody

It also supports the PoET consensus policy, which is commonly used for permissioned architectures. The policy offers low resource utilization along with less computing energy consumption. Nevertheless, the proposed architecture helps multimedia forensics authority and digital forensics engineer to keep track of evidence and protected chain of custody-related information of an asset to be represented in the court of law.

In the proposed architecture, all the case transaction requests are uploaded through the SDK DApp, in which the forensics expert receives the multimedia case records from the forensics authority and forensics engineer. In the beginning, the case records are hash encrypted and stored in the filecoin database, where the system generates meta-information and returns. In the next phase, the forensic expert uploads the transaction proposal request captures all the transactions and forwarded them to all the participating stakeholders. This transaction proposal is received by the sawtooth enabled system validator, where the call processor verifies the proposal and sends back the verification result. After completing the verification process, the system creates a node for the custody of the transaction's evidence chain and verifies it. In the sawtooth state, the transaction's validation must be used for encrypted ledger sync and adds new distributed evidence custody nodes and shares the immutable details in the blockchain network as shown in figure 9 below.

Also, the MF-ledger architecture demonstrates the process of CoC initiated with request case application to the preservation on distributed ledger synchronization through sequence diagram, under distinctly connected participating stakeholders registered, the gain of a distributed system to an incorporative peer network system is apparent. The average result of the proposed architecture implementation returned to the distributed server by the multimedia forensics peer network; also, connection after querying the case transaction of evidence privates' details transparency and traceability maintained. This architecture is also used to evaluate the communication cost between stakeholders, security scalability.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3099037, IEEE Access

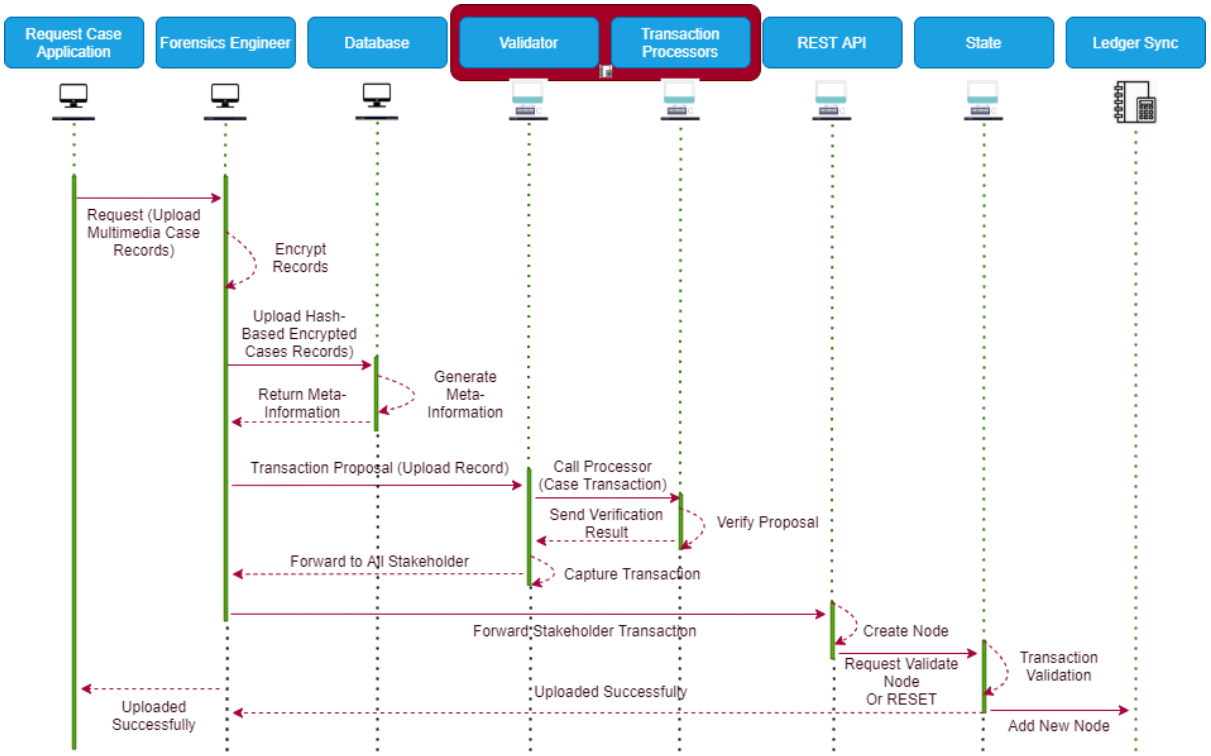

FIGURE 9. **Sequence of all the transaction case application request to transaction validation and Sharing of records among all connected stakeholders**

VI. SAWTOOTH IMPLEMENTATION CHALLENGES

A. COST OF SECURITY, SCALABILITY AND EFFICIENCY

One of the biggest challenges in the implementation of a blockchain network is the cost related to the security scalability and efficiency in the multimedia forensic evidence chain of custody. The sawtooth-enabled architecture achieves provenance and traceability by constantly stimulating distributed ledger when executing transactions and incorporating case details from all the stakeholders. In this way, all the participating stakeholders can see the case-related information on a single go regardless of the individuals who directed the activities. Hyperledger sawtooth avoids each participant's concern to share their operational records with the other stakeholders in the peer network.

B. LACK OF STANDARDIZATION

Within the multimedia forensics investigation systems, there is a diverse range of case investigation procedures contributing to the lack of standardization of multimedia-based evidence chain of custody. The process layer of digital forensics from capturing evidence to preservation is less reliable. This results in unavoidable negative consequences and provides minimal consistent quality. By standardizing the forensics processes, sawtooth architecture enforcing a standard approach and improves the quality of the finished result.

C. RECORD TRANSPARENCY PROBLEM

One of the major challenges is to provide evidence transparency (chain of custody) in a distributed environment. Sawtooth cannot provide a predefined data transparency policy, we have customized sawtooth distributed digital ledger validation and transaction procedure, and consensus verification policy (PoET) that providing a robust infrastructure in terms of privacy protection and security, this can also allow us to build an architecture that preserved information and evidence transparency and traceability of forensics chain of custody investigation. By using the hyperledger sawtooth modularity platform, we enable systems effective record tracking and evidence management at every step of the smart contract. This whole architecture provides enhanced chain custody management, a better transaction registry case, and greater results accuracy compared to the traditional way of digital forensics chain of custody.

D. CHAIN OF CUSTODY DISTRIBUTED STORAGE ISSUES AND CHALLENGES

In the traditional chain of custody management, the only option to preserve the evidence is central storage, leading to data compromise; there is no proper way to resist cyberattacks and making them susceptible to tampering or forgery of evidence. We have used filecone distributed storage structures that connect with the proposed sawtooth architecture and alleviates such limitations by providing automated capture, identifies, examines, analyzes, report, and preserves evidence with smart contracts. And so, these distributed applications deploy a digital contract-based solution aiding both the

multimedia forensics authority and the court of law preserving the chain of custody and in turn the integrity of the evidence.

E. REGULATORY COMPLIANCE ISSUES

Several problems associated with the traditional multimedia forensics evidence chain of custody include errors in the digital case transaction especially record-keeping in centralized storage and relying on third-party security solutions. Adding to that, inappropriate and unreliable tools are used to collect the evidence from portable multimedia devices and its examination and analysis through different forensics techniques.

VII. CONCLUSION

The recent evolution in the technology arena has made the collection, storage, preservation, and analysis of forensic digital evidence an enormously imperative instrument for the resolution of cybercrimes and submitting the evidence in a court of law. Digital evidence and its chain of custody play a vital role in cybercrime investigations, as it links individual events and activities used to perform criminal investigations. In this paper, we introduced the issues and challenges of multimedia-based digital forensics as this information is concealed, volatile, friable, machine/device and time-dependent and can cross jurisdictional borders effortlessly and rapidly. It is, therefore, of utmost importance to assure and guarantee the secrecy, integrity, authenticity and provenance of digital evidence and its chain of custody during cybercrime investigation.

In this paper, we proposed “MF-Ledger”, a blockchain-enabled digital multimedia forensics investigation architecture to bring protection, integrity and tamper-resistance to the digital forensic chain of custody using Hyperledger Sawtooth. The proposed architecture facilitates case-related stockholders to request, access, and record their digital transactions through blockchain DApp on the distributed ledger. Hyperledger Sawtooth a private permissioned blockchain platform is chosen as it provides a modular architecture that separates the distributed core system from the application domain. We created the smart contracts to enable the business logic and accomplish the consensus based on the PBFT consensus policy for core systems fault tolerance and PoET engine to simulate a trust execution environment for attaining the evidence chain of custody. We provide the implementation of the proposed architecture through sequence diagrams and also discussed implementation challenges.

REFERENCES

[1] Dasaklis, T.K., Casino, F. and Patsakis, C., 2020. SoK: Blockchain Solutions for Forensics. arXiv preprint arXiv:2005.12640.

[2] Ahmad, L., Khanji, S., Iqbal, F. and Kamoun, F., 2020, August. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-8).

[3] Karie, N.M., Kebande, V.R., Venter, H.S. and Choo, K.K.R., 2019. On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports*, *1*, p.100008.

[4] Cohen, M., Garfinkel, S. and Schatz, B., 2009. Extending the advanced forensic format to accommodate multiple data sources, logical evidence, arbitrary information and forensic workflow. *digital investigation*, *6*, pp.S57-S68.

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

[6] Kumar, S., Singh, B.K. and Yadav, M., 2020. A Recent Survey on Multimedia and Database Watermarking. Multimedia Tools and Applications, pp.1-49.

[7] Dey, A., Bhattacharya, S. and Chaki, N., 2019. Software watermarking: Progress and challenges. INAE Letters, 4(1), pp.65-75.

[8] Homem, I., 2018. Advancing Automation in Digital Forensic Investigations (Doctoral dissertation, Department of Computer and Systems Sciences, Stockholm University).

[9] Bourouis, S., Alroobaea, R., Alharbi, A.M., Andejany, M. and Rubaiee, S., 2020. Recent Advances in Digital Multimedia Tampering Detection for Forensics Analysis. Symmetry, 12(11), p.1811.

[10] Barrett, D., 2020. Cloud Based Evidence Acquisitions in Digital Forensic Education. Information Systems Education Journal, 18(6), pp.46-56.

[11] Rochmadi, T. and Heksaputra, D., Forensic Analysis in Cloud Storage with Live Forensics in Windows (Adrive Case Study).

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

[13] Bijalwan, A., Solanki, V.K. and Pilli, E.S., 2018. Botnet Forensic: Issues, Challenges and Good Practices. Netw. Protoc. Algorithms, 10(2), pp.28-51.

[14] Jun, M., 2018. Blockchain government-a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity, 4(1), p.7.

[15] Karie, N.M., Kebande, V.R. and Venter, H.S., 2019. Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International: Synergy, 1, pp.61-67.

[16] Li, D., Liu, W., Deng, L. and Qin, B., 2020. Design of multimedia blockchain privacy protection system based on distributed trusted communication. Transactions on Emerging Telecommunications Technologies.

[17] Bhowmik, D. and Feng, T., 2017, August. The multimedia blockchain: A distributed and tamper-proof media transaction framework. In 2017 22nd International Conference on Digital Signal Processing (DSP) (pp. 1-5). IEEE.

[18] Uddin, M. (2021). Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics*, *597*, 120235.

[19] Xiong, Y. and Du, J., 2019, January. Electronic evidence preservation model based on blockchain. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (pp. 1-5).

[20] Kumar, M.R. and Bhalaji, N., 2020. Blockchain Based Chameleon Hashing Technique for Privacy Preservation in E-Governance System. Wireless Personal Communications, pp.1-20.

[21] Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q., 2020. A survey on the security of blockchain systems. Future Generation Computer Systems, 107, pp.841-853.

[22] Lusetti, M., Salsi, L. and Dallatana, A., 2020. A blockchain based solution for the custody of digital files in forensic medicine. Forensic Science International: Digital Investigation, 35, p.301017.

[23] Nyaletey, E., Parizi, R.M., Zhang, Q. and Choo, K.K.R., 2019, July. BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 18-25). IEEE.

[24] Jeong, J., Kim, D., Lee, B. and Son, Y., 2020. Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric. Journal of Information Processing Systems, 16(4).

[25] Al-Khateeb, H., Epiphaniou, G. and Daly, H., 2019. Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In Blockchain and Clinical Trial (pp. 149-168). Springer, Cham.

[26] Lone, A.H. and Mir, R.N., 2018. Forensic-chain: ethereum blockchain based digital forensics chain of custody. Sci. Pract. Cyber Secur. J.

[27] Bonomi, S., Casini, M. and Ciccotelli, C., 2018. B-coc: A blockchain-based chain of custody for evidences management in digital forensics. arXiv preprint arXiv:1807.10359.

[28] Li, M., Lal, C., Conti, M. and Hu, D., LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Generation Computer Systems, 115, pp.406-420.

[29] Zarpala, L. and Casino, F., 2020. A blockchain-based Forensic Model for Financial Crime Investigation: The Embezzlement Scenario. arXiv preprint arXiv:2008.07958.

[30] [Chopade, M., Khan, S., Shaikh, U. and Pawar, R., 2019, December. Digital Forensics: Maintaining Chain of Custody Using Blockchain. In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 744-747). IEEE.

[31] Nasir, Q., Qasse, I.A., Abu Talib, M. and Nassif, A.B., 2018. Performance analysis of hyperledger fabric platforms. Security and Communication Networks, 2018.

[32] Soltani, R., Nguyen, U.T. and An, A., 2018, July. A new approach to client onboarding using self-sovereign identity and distributed ledger. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1129-1136). IEEE.

[33] Hasan, H.R., Salah, K., Jayaraman, R., Omar, M., Yaqoob, I., Pesic, S., Taylor, T. and Boscovic, D., 2020. A Blockchain-Based Approach for the Creation of Digital Twins. IEEE Access, 8, pp.34113-34126.

[34] Elrom, E., 2019. Hyperledger. In The Blockchain Developer (pp. 299-348). Apress, Berkeley, CA.

[35] Takemiya, M. and Vanieiev, B., 2018, July. Sora identity: secure, digital identity on the blockchain. In 2018 ieee 42nd annual computer software and applications conference (compsac) (Vol. 2, pp. 582-587). IEEE.

[36] Ampel, B., Patton, M. and Chen, H., 2019, July. Performance modeling of hyperledger sawtooth blockchain. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 59-61). IEEE.

[37] Shi, Z., Zhou, H., Hu, Y., Jayachander, S., de Laat, C. and Zhao, Z., 2019, June. Operating Permissioned Blockchain in Clouds: A Performance Study of Hyperledger Sawtooth. In 2019 18th International Symposium on Parallel and Distributed Computing (ISPDC) (pp. 50-57). IEEE.

[38] Verdoliva, L. and Bestagini, P., 2019, October. Multimedia Forensics. In Proceedings of the 27th ACM International Conference on Multimedia (pp. 2701-2702).

Abdullah Ayub Khan is a PhD scholar at Faculty of Computer Science at Sindh Madressatul Islam University Karachi. Mr. Abdullah has published around 10 research papers in well-reputed journals in the domain of digital forensics, network security and artificial intelligence.

Dr Mueen Uddin is currently working as Assistant Professor of Cybersecurity and Blockchain at Universiti Brunei Darussalam. He completed his PhD from Universiti Teknologi Malaysia UTM in 2013. Dr. Mueen has authored more than 90 International research articles published in highly indexed and reputed journals. His research interests include Blockchain, cybersecurity, cloud computing and virtualization.

Dr. Aftab Ahmed Shaikh has earned his Doctorate Degree in Computer Application & Technology from Beijing University of Aeronautics and Astronautics (BUAA) in 2010. He has more than Eighteen years of professional experience in teaching and research in different countries including Pakistan, China, and Oman. He is associated with a number of reputable research communities and editorial boards. Dr. Aftab is a well-published author of several research articles in reputable international Journals and Conference Proceedings. He has supervised several dissertations and projects and leading a research group of Computational Intelligence (CI).

Dr. Asif Ali Laghari earned his Ph.D. in Computer Science & Technology from Harbin Institute of Technology (HIT), China in 2019. He is the author of over 55 research articles in HEC recognized and impact factor journals, conferences, and two book chapters of international repute. His research interests include Cloud Computing, Quality of Experience, Multimedia streaming, Fog computing, and Social Networking.

Dr. Adil E. Rajput is currently working as Assistant Professor at Computer Science Department Effat University Jeddah KSA. He earned his PhD from George Washington University USA. He has authored many international publications in highly reputable journals and conferences.