IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 20 June 2023, accepted 2 August 2023, date of publication 7 August 2023, date of current version 10 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3302771

RESEARCH ARTICLE

Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain

SUMIT KUMAR RANA[1], ARUN KUMAR RANA[2], SANJEEV KUMAR RANA[3], VISHNU SHARMA[2], (Member, IEEE), UMESH KUMAR LILHORE[4], OSAMAH IBRAHIM KHALAF[5], AND ANTONINO GALLETTA[6], (Member, IEEE)

[1]Department of Computer Science and Engineering, Panipat Institute of Engineering and Technology, Panipat 132102, India
[2]Department of Computer Science and Engineering, Galgotia College of Engineering, Greater Noida, Uttar Pradesh 201310, India
[3]Department of Computer Science and Engineering, Maharishi Markandeshwar (Deemed to be University), Ambala, Haryana 133203, India
[4]Department of Computer Science and Engineering, Chandigarh University, Sahibzada Ajit Singh Nagar, Punjab 140413, India
[5]Department of Solar, Al-Nahrain Research Center for Renewable Energy, Al-Nahrain University, Jadriya, Baghdad 10070, Iraq
[6]MIFT Department, The University of Messina, 98166 Messina, Italy

Corresponding author: Antonino Galletta (angalletta@unime.it)

This work was supported in part by the Department for Drug Policies, Presidency of the Council of Ministers, Italian Government, through the Project InstradaME, under Grant CUP F49I20000100001; in part by the National Operational Program Metropolitan Cities 2014–2020 [Piano Operativo Nazionale Città Metropolitane (PON METRO)] through the Project Agor'a under Grant CUP F41I17000170006; in part by the Cloud@ME Project under Grant CUP F49E17000040006; in part by the ImpleME Project under Grant CUP F41I17000180006; in part by the MeSm@rt Project under Grant CUP F41I18000230006; and in part by the Urbamid+ Project under Grant CUP F41H18000030006.

ABSTRACT Modern legal proceedings heavily rely on digital evidence as a basis for decisions in a variety of contexts, including criminal investigations and civil lawsuits. However, factors like data alteration, unauthorised access, or flaws in centralised storage can threaten the security and integrity of digital evidence. We suggest a decentralised methodology for using smart contracts to safeguard digital evidence in order to overcome these issues. The decentralised model makes use of smart contracts and blockchain technology to guarantee the integrity, transparency, and immutability of digital evidence. The approach does not require a centralised authority because it makes use of a distributed ledger, which lowers the possibility of data loss or manipulation. Multiple parties participating in the evidence lifecycle can build confidence and accountability thanks to smart contracts' programmable rules and automated enforcement mechanisms. In our study, we show the decentralised model's architecture and describe its essential elements, such as the blockchain network, smart contracts, and decentralised storage. We go over the advantages of employing this architecture, including enhanced auditability, decreased dependency on centralised institutions, and increased data security. Additionally, we discuss potential difficulties and constraints, like scalability and interoperability. We run a few simulations and experiments to test the suggested model's viability and effectiveness while comparing it to conventional centralised methods. The outcomes show that our decentralised paradigm offers improved security for digital evidence, guaranteeing its reliability, usability, and tamper-proofness. We also go through how the model is used in actual legal systems, law enforcement organisations, and digital forensics investigations.

INDEX TERMS Blockchain technology, digital forensic, distributed ledger technology, IPFS.

I. INTRODUCTION

The use of digital evidence in court cases in many different fields has grown increasingly important in the current digital era. In criminal investigations, civil lawsuits, and regulatory compliance, digital evidence—such as electronic documents,

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Guidi.

recordings, and transaction records—forms the basis for decision-making [1]. However, there are many threats to the integrity and security of digital evidence, such as data manipulation, unauthorised access, and flaws in centralised storage systems. We present a research paper that introduces a decentralised model using smart contracts on the Polygon blockchain to safeguard digital evidence in order to allay these worries. To protect the validity, immutability, and accessibility of digital evidence, the decentralised solution we suggest makes use of blockchain technology, specifically the Polygon blockchain [2]. The scalability and low transaction costs of the Polygon blockchain make it the perfect platform for deploying decentralised applications. The concept creates a framework that assures trust, openness, and accountability throughout the lifecycle of digital evidence by utilising the capabilities of smart contracts [3].

In this article, we go over our decentralised model's architecture and essential elements. We go into the details of the Polygon blockchain, emphasising how well it fits our research goals. We look at how smart contracts, which offer programmable rules and automatic enforcement mechanisms, facilitate the safeguarding of digital evidence. Our methodology provides improved security and dependability for digital evidence management by integrating smart contracts with the Polygon blockchain [4], [5], [6].

We consider the advantages of using our decentralised paradigm in contrast to conventional centralised methods. Our model lowers the danger of data modification and unauthorised access by eliminating the reliance on a single, centralised authority. The integrity of digital evidence is guaranteed by the blockchain's transparency and immutability, making it tamper-proof and verifiable [7]. Additionally, our model's decentralised storage infrastructure improves accessibility and lowers the risk of data loss.

We outline the benefits of our decentralised model while also acknowledging its drawbacks [8]. In blockchain-based systems, scalability and interoperability are crucial factors. We explore these issues and suggest solutions to effectively overcome them, assuring the applicability and usability of our model in actual situations. To evaluate the feasibility and effectiveness of our proposed decentralized model, we conduct experiments and simulations, focusing on the integration of smart contracts with the Polygon blockchain [7], [8]. We compare the performance and security of our model with traditional centralized approaches, analysing metrics such as data integrity, accessibility, and system robustness. The results of our experiments demonstrate the superiority of our decentralized model in protecting digital evidence and validate its potential applicability in legal systems, law enforcement agencies, and digital forensics investigations. Fig. 1 shows the conventional evidence collection and management process.

A. PROBLEM STATEMENT

All the traditional approaches were centralized in nature, which typically encounter issues such as single points of failure and lack of confidence. Centralized methods are not suitable for collaborative settings as trust issues often emerge. Therefore, a decentralized strategy is required to operate in a collaborative environment. The absence of a mediator in this decentralized approach resolves the trust problem and reduces costs. Consequently, a decentralized model is proposed to ensure security and trust in the judicial process.

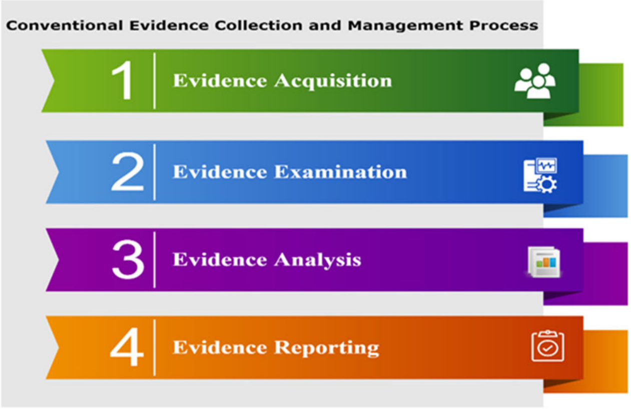


FIGURE 1. Conventional evidence collection and management process.

B. MOTIVATION AND CONTRIBUTIONS

This paper discusses how blockchain technology can improve privacy and security in the judicial domain. In this domain, distributed ledger technology can help maintain the security, integrity, and authenticity of evidence, which plays a crucial role in judicial proceedings. Therefore, handling evidence with extra care is essential. This article investigates the potential applications of distributed ledger technology in the judicial domain and presents the following contributions:

- Discovery of several problems in the judicial domain and discussion of the advantages of integrating distributed ledger technology in this domain.
- Proposal and implementation of a blockchain-supported decentralized access control solution, which can be adapted for use with other blockchain frameworks.
- Use of proof of stake at the blockchain level and proof of authority at the application level. Only a few pre-selected nodes have the authority to approve or reject transactions, reducing the time required to create blocks compared to the previous approach.

The structure of the paper is as follows: Section II reviews related work by different authors to gain insights into the judicial domain. Section III elaborates on the problems with the traditional judicial approach. Section IV describes the role of blockchain technology. The proposed model and its workflow are presented in Section V, while Section VI showcases the implementation of the proposed model. The advantages of the proposed model are discussed in Section VII. Section VIII explores the research implications, and finally, the article concludes in Section IX.

II. RELATED STUDY

Digital data analysis for forensics and digital investigations is in high demand as society becomes increasingly dependent on digital technologies. The rapid adoption and widespread use of digital technologies have led to an increase in cybercrimes. Consequently, the utilization of digital forensics systems has become necessary to collect, analyse, and present evidence while ensuring its admissibility in court. The ability of distributed ledger technology to prevent tampering has led to its application in other fields where data integrity must be preserved.

This article presents a paradigm that enables the assessment of the credibility of digital evidence based on information. The digital evidence is stored on a blockchain, which is accessible to authorized individuals. The reliability and applicability of the digital evidence are evaluated by the relevant parties involved. Additionally, a data structure called the Global Digital Timeline has been developed to record the chronological sequence of activities throughout the lifecycle of the evidence. The model primarily focuses on ensuring the traceability and non-repudiation of the evidence [9].

This article describes a novel framework that integrates Software-Defined Networking (SDN) and the Internet of Things (IoT) to support the forensic domain. The proposed framework was evaluated using a network simulator. In this framework, the gateway forwards packets from each IoT device to switches. Once the device signatures are verified, the packets reaching the control plane are classified. The SDN controller utilizes blockchain to validate data packet signatures prior to classification. These packets contain information such as the user's name, source and destination IP addresses, local time of the evidence occurrence, location of occurrence, and the corresponding action taken. Forensics investigators with proper authorization can access the data stored in the SDN controllers. The hexadecimal hash value of the evidence is stored to maintain a high level of dependability in the chain of custody (CoC) and to preserve the confidence and integrity of the evidence [10].

Author proposed the utilization of LedgerDB on Alibaba Cloud as an alternative to decentralized architectures, where they were not strictly necessary. In such cases, system performance can be limited, leading to low throughput, high latency, and significant storage overhead. LedgerDB is a centralized ledger database designed to provide features similar to blockchain, such as tamper-evidence and non-repudiation, while offering enhanced performance. It ensured strong auditability through the implementation of a TSA two-way peg protocol, which effectively prevents malicious behavior from both users and service providers. Additionally, LedgerDB supports the removal of verifiable data, which was often required in real-world applications to eliminate outdated records for storage efficiency or to hide certain records for regulatory compliance, all while maintaining its verifiability. Through experimental evaluation, they have found that LedgerDB exhibits a throughput that is 80 times higher than state-of-the-art permissioned blockchains like Hyperledger Fabric. As a result, many customers utilizing blockchain applications, such as IP protection and supply chain, on Alibaba Cloud have transitioned to LedgerDB due to its advantages in terms of high throughput, low latency, strong auditability, and user-friendly interface [11].

Different methods and techniques are required to maintain the integrity of evidence during the investigation process. To acquire digital evidence and address security concerns in the context of smart homes, a management system was designed. This system offered intelligence, automated discovery, and innovative information recording capabilities [12].

The authors examined the importance of video evidence in investigations. However, tampering with video evidence posed a significant challenge. The authors suggested a blockchain-based integrity verification mechanism. In this paradigm, a video integrity code was generated using a hash-based mechanism. If any of the video segments are tampered with, this integrity code would be altered. By comparing the two video integrity codes, manipulation can be quickly identified. Comparative investigations have demonstrated that the proposed model performs better for the security of video evidence [13].

The authors proposed a model for gathering evidence from a cloud environment. This concept utilizes distributed ledger technology and Software-Defined Networking (SDN) to preserve the evidence. Additionally, a new algorithm was developed to secure the collected data. Java and NS3 were used to simulate the entire system. The evaluation analysis of the proposed model demonstrated its effectiveness compared to a centralized approach [14].

Researchers have developed a method for IoT forensics that aims to protect the confidentiality of personal information provided by individuals. The discussed strategy has been implemented using the PRoFIT methodology. The research focused on a paradigm for collecting digital evidence in IoT environments. This strategy has been tested in multiple settings with varying privacy requirements, and the assessment has demonstrated that the proposed methodology successfully balances the ideals of IoT-based research and secrecy [15].

This paper introduces a novel approach for secure and tamper-proof storage of Electronic Health Records (EHRs) in a cloud environment using blockchain technology. The proposed strategy ensures the infeasibility of tampering with outsourced EHRs within distributed IPFS nodes. Additionally, it guarantees the computational unforgeability of the stored EHRs. The model addresses the risk of collusion between malicious doctors and the Cloud Service Provider (CSP) to manipulate the outsourced EHRs. Implementation of the model leverages the Ethereum blockchain, integrating the generated EHRs into transactions for enhanced integrity. By following the computational intractability of Ethereum, the model preserves the timeliness of the outsourced EHRs, allowing for efficient extraction of their generation time. Security analysis demonstrates the model's resilience against various attacks on distributed IPFS nodes at the CSP. A comprehensive numerical evaluation and comparison of experimental results validate the practicality and effectiveness of the proposed model, particularly in terms of computation and communication overhead [16].

The researchers examined various information formats, types of forensic evidence, and other complexities in the IoT ecosystem. Their primary goal was to gather data and artifacts from different IoT network-connected devices. After collecting the artifacts and data, the researchers analysed the interrelation of the evidence before entering it into a blockchain-based forensic model [17].

The problems that can occur while using a centralised network for transferring or storing patient medical data have been studied by researchers. They have noted a number of issues, such as a lack of historical data, erroneous access, and confidentiality issues. The authors have created a paradigm that blends blockchain technology with encryption to address these problems. According to this paradigm, all data is accessible only with the consent of the parties concerned and all information is provided with their consent [18].

The needs of numerous parties engaged in gathering digital evidence have also been investigated by the researchers. They understand the value of a system that can guarantee the reliability of the proof offered in court. As a result, they have developed a system that collects, stores, and shares evidence with stakeholders using blockchain technology and smart contracts. In this paper, the usefulness of the suggested system has also been explored [19].

The writers have looked at how blockchain technology is being used in the legal industry. They have acknowledged that the integrity and confidence in the process of acquiring and sharing evidence may be preserved by blockchain's fundamental properties, such as provenance, transparency, and decentralisation. The authors have suggested a blockchain-based system for producing electronic evidence, allowing judicial institutions to confirm the validity of evidence used in court cases. System analysis shows that the suggested system gives the application area provenance, trust, and efficiency [20].

The researchers have shown that simply hashing data does not provide sufficient data security because it does not record the time the hash was generated. Consequently, a technique for timestamped hashing is required. To avoid data alteration and improve data transparency, the researchers have devised a blockchain-based approach that makes use of public blockchains. This enables diverse court participants to keep track of and evaluate the evidence whenever they choose. This model can serve as a cornerstone for new researchers in the same field [21].

The authors have examined the utilization of blockchain technology for the medical research community. They have presented a paradigm for storing and querying pharmacogenomics data, which was implemented using the Ethereum blockchain and a solidity-based smart contract. According to algorithm analysis, the proposed model was efficient and reduced query time, even with a query pool of 10,000 queries. The algorithm was designed considering solidity constraints, such as variable quantity and gas requirements. The method used in this model has shown success in the medical industry, and the authors express optimism about its potential application in other fields for future research [22].

This paper examines the relationship between the right to a fair trial as defined in Article 6 of the European Convention on Human Rights (ECHR), its interpretation in case law, and its relevance to evidence law, particularly during the investigative phase of criminal proceedings. The analysis aims to shed light on how this principle implicitly establishes a foundation for the establishment of universal rules pertaining to evidence. Within this framework, two distinct groups of evidence rules are identified: those based on the principle of equality of arms and those based on the presumption of innocence. The paper outlines and discusses specific challenges that arise in the context of digital investigations for each of these groups. Furthermore, it explores the implications within a new governance model for digital evidence [23].

III. PROBLEMS WITH TRADITIONAL JUDICIAL APPROACH

In traditional approach, a form is filled manually to store all the activities that had happened with the evidences from its collection to the time of submission in the court [24]. Following information can be recorded as and when the evidence moves with the investigation process:

- Date and place of origin of the evidence.
- Physical description of the evidence.
- When, how long and who handled the evidence with all the details.
- Unique identification for each person involved in the investigation
- Process by which evidence was transferred from one person to another person.

The following discussion focuses on a few factors that can prevent crucial evidence from being admitted into court, rendering it legally useless.

Plaintiffs may use an advocate to submit a complaint under the present judicial system. Legal procedures result in high costs for the average person since they are not well understood by him. He must therefore completely rely on the advocates [25]. This irrational faith could have a variety of negative effects, like cheating on him, making unnecessary purchases, etc.

Accountability: Because they will claim work stress as an excuse, no court official will accept responsibility for the delay in court procedures. But in the end, it will be the average person who suffers [26].

Provenance: Evidence is susceptible to manipulation. We are unable to go back and look at the evidence using the existing system [27].

Transparency: Because there is a lack of openness in the current system, court officials may abuse information without other stakeholders' knowledge [28].

Data Integration: The court system keeps track of the records for each zone. Therefore, it is challenging to integrate records when a case covers many zones [29].

Scalability: Scalability will be a problem to handle the legal procedure if the case spans numerous states or nations [30].

A solution is required that can address the aforementioned problems and aid in the management and submission of evidence. The technology that can assist in reaching this goal is blockchain.

IV. ROLE OF BLOCKCHAIN TECHNOLOGY

As demonstrated in Fig. 2, a blockchain is a chain of blocks that are linked together using the hashing algorithm. A distributed ledger supported by blockchain technology is notable for being unchangeable, impenetrable, and decentralized.

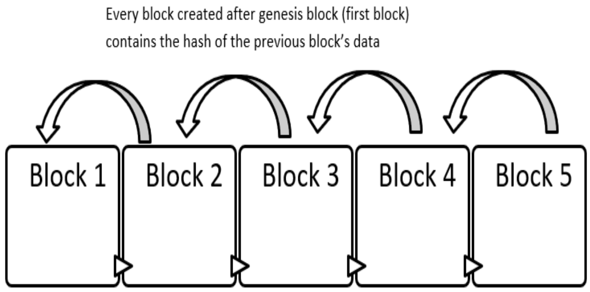

Every block created after genesis block (first block)
contains the hash of the previous block's data
Block 1
Block 2
Block 3
Block 4
Block 5

FIGURE 2. **Conceptual illustration of blockchain.**

The authors conducted research on common practices for sharing medical records. Traditional methods were found to have various issues, including privacy concerns, data centralization, and trust challenges. Therefore, the authors focused on blockchain-supported methods for sharing medical data. They examined both public and private blockchains and explored potential research topics related to blockchain-based medical data exchange [31].

The framework for every blockchain-supported application is built upon principles such as transactions, peer-to-peer networks, consensus algorithms, decentralized ledgers, and smart contracts. Transactions refer to any form of communication or interaction between peer-to-peer network nodes. Examples include cryptocurrency transfers, file ownership, data storage, and data access [32]. A peer-to-peer network is a network of nodes with the same capabilities or resources, where there is no distinction between client and server. The consensus algorithm is the method used by peer-to-peer network nodes to decide whether to approve or reject a given transaction in the network. All nodes in the peer-to-peer network have access to the decentralized ledger, which records all transactions through consensus [33].

A smart contract is a computer software designed to support agreements between parties that can communicate, and it is triggered by specific system events. Blockchain technology has various applications in industries such as insurance and digital asset management. One notable example is its impact on the legal system, where the distributed ledger technology securely stores documents in digital form. This is enabled by peer-to-peer networks that facilitate data sharing and exchange among all parties [34]. All information is securely encrypted, and the ledger provides complete transparency by documenting every data access. Any attack on data integrity can be traced and verified. A model is proposed that combines back-end data storage with blockchain technology. Digital evidence can be stored in the data storage, while the blockchain is used to record all evidence access transactions.

V. PROPOSED MODEL

In the proposed model, distributed ledger technology is employed to provide security to the evidences by using Ethereum blockchain and IPFS. Let us discuss about the various concepts of the model and work flow of the proposed model.

A. SYSTEM MODEL

The key components of the proposed model are judicial evidences, polygon blockchain (Mumbai testnet), interplanetary file system for data storage at back end and various users of the system. Above mentioned components are connected in such a way that information can be exchanged among them as per requirement. Let us discuss these components.

- Judicial Evidences: Judicial evidences are the documents that are used as a proof for the fair judgement in any court case. This is the most significant component of the proposed model. Various entities will access evidences during a court case processing. Security and integrity of these evidences are the main objective because tampered or manipulated evidences can lead to wrong judgement [35]. These wrong decisions can hurt the belief on the judicial system. So, a decentralized and transparent system is built with the help of polygon blockchain (Mumbai testnet).
- Polygon Blockchain (Mumbai Testnet): Decentralization of powers is required to build a trusted and transparent system. This decentralization can be achieved with the help of a polygon blockchain (Mumbai testnet). It has a distributed ledger which is shared among all the stakeholders of the peer-to-peer network. All the transactions like upload, delete or access are stored in this ledger. This ledger is immutable which means once something is written on the ledger then it cannot be changed or deleted. Mumbai Testnet, which is used for testing, duplicates the Polygon Mainnet. The faucet offers testnet tokens for users to purchase. In contrast to assets that have value, like MATIC, testnet tokens have no value [36]. This enables programmers or network administrators to test setups and try out other implementations. As the block size of the blockchain is very small so evidences cannot be stored on it. So, inter planetary file system is used to satisfy our off-chain storage needs.
- IPFS: As our objective is to build a decentralized system so we also need a storage mechanism which is not centralized.

InterPlanetary File System can be employed to cater this need. IPFS stores the data in a distributed manner by using nodes present at different geographical locations. When any data is stored on this storage system, a unique hash is returned which is known as the content address (CID) of the document. This CID can be used to retrieve the file in near future. Same CID is returned if files with same data is uploaded so it also avoids data duplication. Judicial evidences will be stored on ipfs in proposed model [37].

- System User: Users of this proposed system will be any official from police department, prosecution lawyer, defense lawyer etc. every stakeholder has a pair of keys which are used while retrieving the evidences connected to a particular case. These keys will authenticate the user and avoids repudiation.

B. WORK FLOW

In the proposed model we have different entities like creator Admin, Super Admin, Admin, User. Work flow of the process is shown in Fig. 3

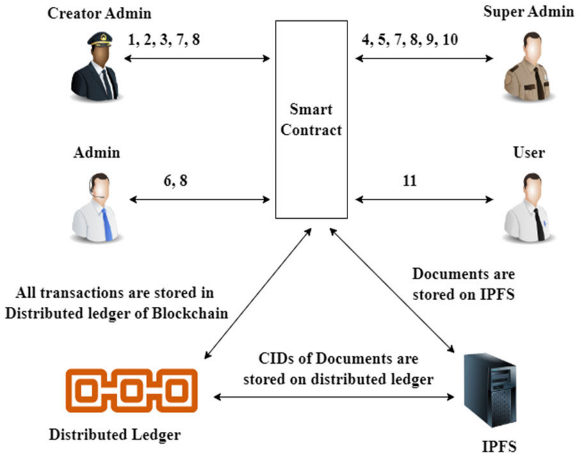

Creator Admin
1, 2, 3, 7, 8
Super Admin
4, 5, 7, 8, 9, 10
Smart Contract
Admin
6, 8
User
11
All transactions are stored in Distributed ledger of Blockchain
Documents are stored on IPFS
CIDs of Documents are stored on distributed ledger
Distributed Ledger
IPFS

FIGURE 3. Work flow of entities creation and approval process.

1. Smart contract is deployed by the creator admin. Functional view is generated.

2. Creator admin creates super admin.

3. Creator admin approves super admin. Because Super admin entity will be able to use his power after the approval from creator admin.

4. Approved super admin can add new admin.

5. Creator admin or approved super admin approves new admin. Admin cannot create a new admin.

6. Approved admin creates a new user but it cannot approve it.

7. New user can be approved by a creator admin or an approved super admin. new user cannot create evidence.

8. Creator admin, approved super admin and approved admin can create evidence.

9. Every newly created evidence is approved or rejected by the approved super admin. Only owner of the evidence can change the ownership of the evidence.

10. This ownership change is approved or rejected by the approved super ad-min.

11. A user can only get the ownership of any evidence if he is an approved user. User needs ownership of evidence before he can access the evidence.

```
Algorithm: Creation and Approval of New Evidence Record
If (msg.sender = user)
Then "evidence can't be created and operation declined"
Elseif ((msg.sender = $\text{Admin}_{\text{creator}}$) or( msg.sender =
  $\text{Admin}_{\text{verified-super}}$) or( msg.sender = $\text{Admin}_{\text{verified}}$))
Then "Evidence can be created but not yet approved"
For approval of evidence, If (msg.sender = Evidence
  owner)
    Then "operation declined"
Elseif ((msg.sender = $\text{Admin}_{\text{creator}}$) or( msg.sender =
  $\text{Admin}_{\text{verified-super}}$) or( msg.sender = $\text{Admin}_{\text{verified}}$))
Then "Evidence can be approved"
Else "operation declined"
```

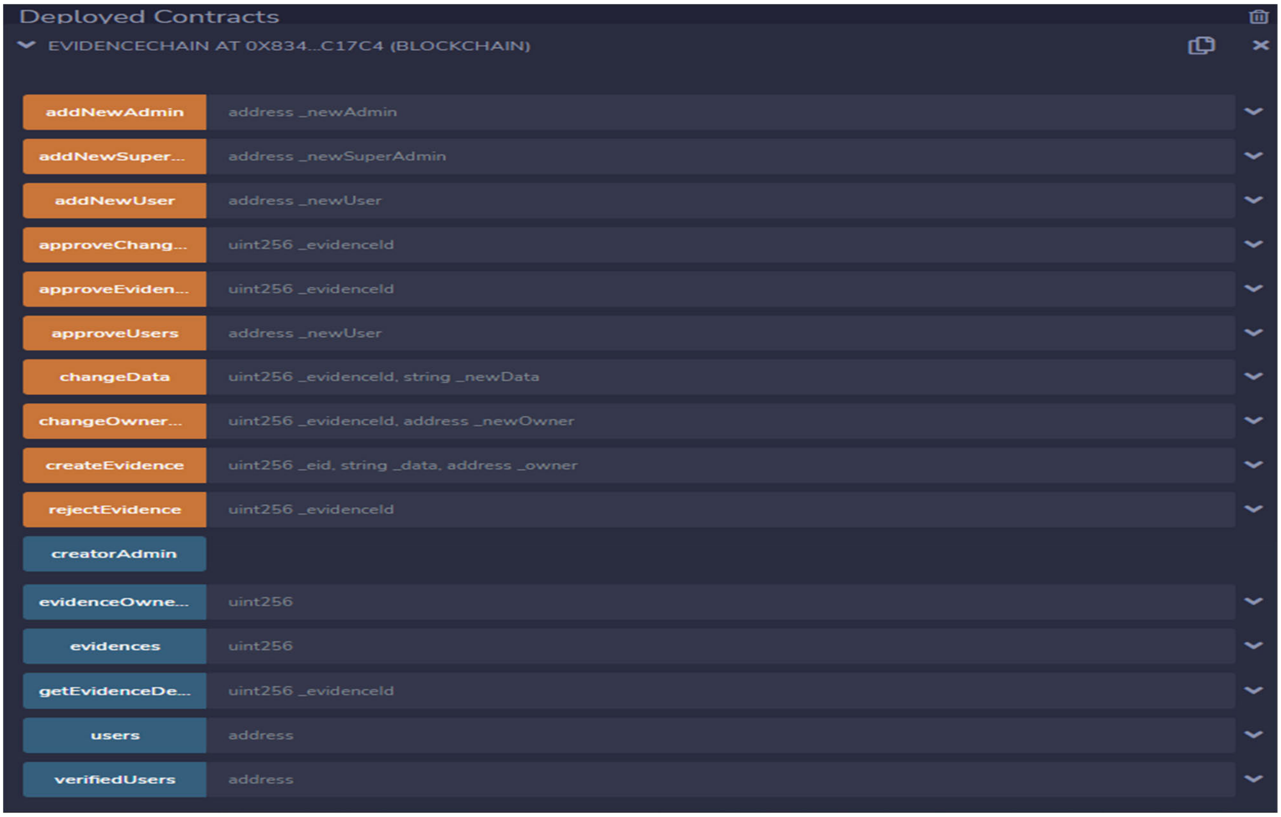
All related documents are stored on IPFS. When a document is stored on IPFS, CID of the document will be returned. This CID is stored on the distributed ledger in form of a transaction. Algorithms for the processes are given below.

```
Algorithm: Add New Admin
Contract deployed by Creator Admin/verified Super
  Admin with value 3
If ((msg.sender = $\text{Admin}_{\text{creator}}$) or( msg.sender =
  $\text{Admin}_{\text{verified-super}}$))
    Then " new admin can be added with value 2 but not yet
  approved"
Else "new admin can't be added and operation declined"
For approval, If ((msg.sender = $\text{Admin}_{\text{creator}}$) or(
  msg.sender = $\text{Admin}_{\text{verified-super}}$))
    Then "new Admin can be approved"
Else "new admin can't be approved and operation
declined"
```

VI. TOOLS AND IMPLEMENTATION

Tools that are used for the implementation of the proposed model are:

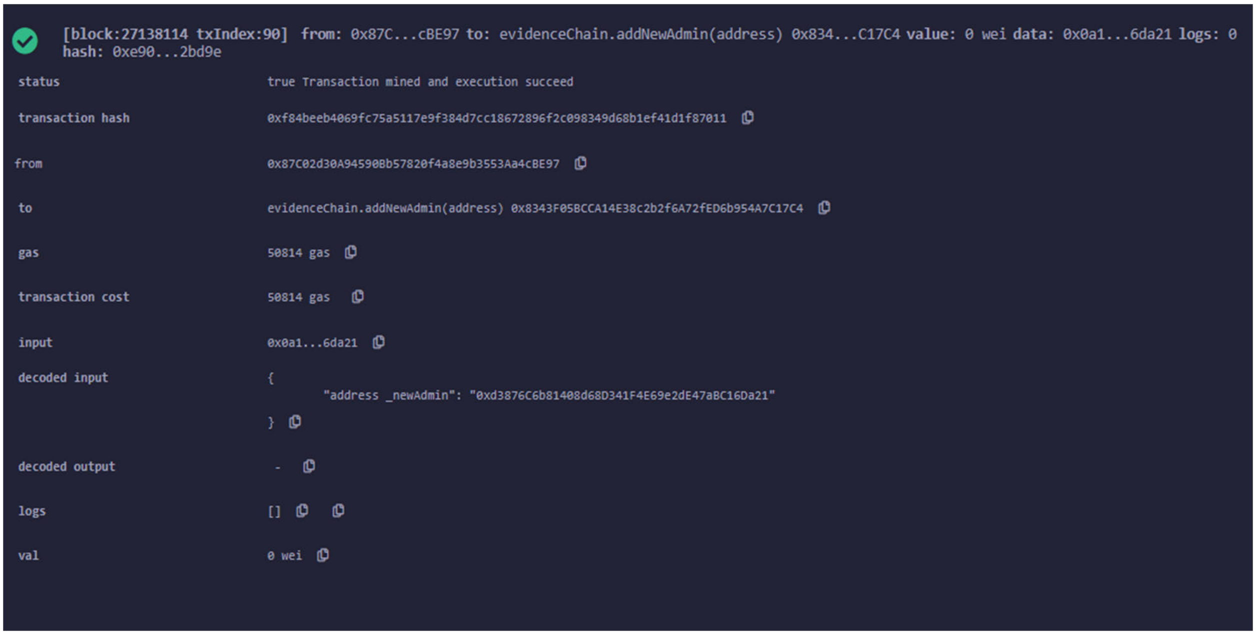
- Remix IDE: This IDE is used for the development and deployment of smart contract. Smart contract are the programs written in solidity that contains the logic which controls the access to the digital assets.
- Meta mask: This is a cryptocurrency wallet. It maintains the account of the users. All the transactions are confirmed from this wallet before the execution.
- Ganache: It is used to provide a local blockchain environment on our system. It provides us with ten dummy accounts to test proposed model on our system.



```
Deployed Contracts
EVIDENCECHAIN AT 0X834...C17C4 (BLOCKCHAIN)

addNewAdmin          address _newAdmin
addNewSuper...       address _newSuperAdmin
addNewUser           address _newUser
approveChang...      uint256 _evidenceId
approveEviden...     uint256 _evidenceId
approveUsers         address _newUser
changeData           uint256 _evidenceId, string _newData
changeOwner...       uint256 _evidenceId, address _newOwner
createEvidence       uint256 _eid, string _data, address _owner
rejectEvidence       uint256 _evidenceId
creatorAdmin
evidenceOwne...      uint256
evidences            uint256
getEvidenceDe...     uint256 _evidenceId
users                address
verifiedUsers        address
```

FIGURE 4. View after deployment of smart contract.



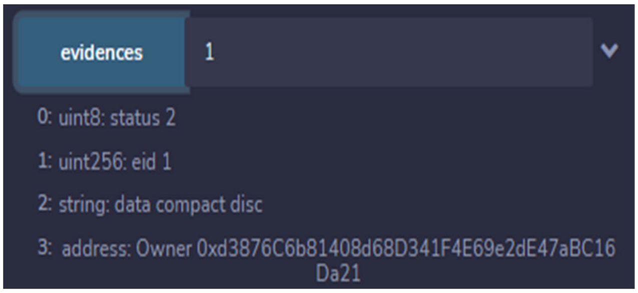
```
[block:27138114 txIndex:90] from: 0x87C...cBE97 to: evidenceChain.addNewAdmin(address) 0x834...C17C4 value: 0 wei data: 0x0a1...6da21 logs: 0
hash: 0xe90...2bd9e
status              true Transaction mined and execution succeed
transaction hash    0xf84beeb4069fc75a5117e9f384d7cc18672896f2c098349d68b1ef41d1f87011
from                0x87C02d30A94590Bb57820f4a8e9b3553Aa4cBE97
to                  evidenceChain.addNewAdmin(address) 0x8343F05BCCA14E38c2b2f6A72fED6b954A7C17C4
gas                 50814 gas
transaction cost    50814 gas
input               0x0a1...6da21
decoded input       {
                            "address _newAdmin": "0xd3876C6b81408d68D341F4E69e2dE47aBC16Da21"
                    }
decoded output       -
logs                []
val                 0 wei
```

FIGURE 5. Transaction details of addNewAdmin function of smart contract.

- Polygon Blockchain (Mumbai Testnet): It provides global blockchain environment. It consists of a main network and test network. Main network is used for final deployment of any blockchain based application. It requires real cryptocurrency Matic. So, for testing of proposed model, test networks are used.

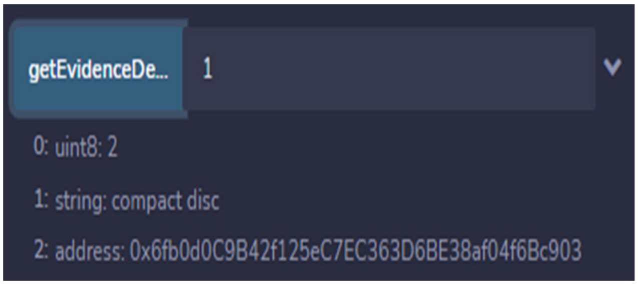
- IPFS: Interplanetary file system is a decentralized file system which is used to store the files or documents. When a file is stored on ipfs a content identifier (CID) is generated corresponding to this file. If this file is modified by anybody then its CID will also change. For two identical file same CID is generated.

To implement the proposed model, first we add Mumbai test network in our Metamask wallet. Network name is Mumbai testnet with chain id 80001 and RPC URL as https://rpc-mumbai.maticvigil.com/. After adding, we can find this testnet in our wallet. Then we create few accounts which are used during the implementation. Then to deploy our smart contract on polygon test network we require test token MATIC. We add these test tokens in our account from the polygon faucet. After adding some test token in our accounts, we deploy our smart contract with the help of Remix IDE. This contract deployment transaction is passed to Metamask for confirmation. After the confirmation and contract is deployed on polygon Mumbai testnet. The view after deployment of contract is shown in Fig. 4. The functions in our contract are shown in two colours. Functions with an orange colour are those that can change the value of some data. The functions with a blue colour can only read the data and cannot modify it. Then, we try to add a new admin by passing the hexadecimal address of the account to the addNewAdmin function. Only the creator admin and approved super admin have the power to add admin. Transaction details are shown in Fig. 5. We can check the user details by passing the hexadecimal address to the users function, and the status level is 2 as indicated in the decoded output. Before attaining the power of an associated role, a user must be approved. The hexadecimal address of the newly added admin is passed to the verifiedUsers function, and the received response shows that the approval status is false. Then, this newly created admin is approved by the approved super admin using the approveUsers function. If the hexadecimal address of the newly created admin is passed to the verifiedUsers function, the approval status is true. If a user who is not approved tries to create evidence, the transaction is declined. Then, this user is approved by the approved super admin using the approveUsers function. After approval, if the same user tries to create evidence, the transaction is executed successfully. Only the creator admin, approved super admin, and approved admin have the power to create new evidence. Normal users cannot create evidence. The details of this newly created evidence can be checked using the getEvidenceDetails function. You can see the evidence ID, data related to the evidence, and the address of the evidence owner. The status of the evidence is 1, which means it is not yet approved. Only the approved super admin has the power to approve any evidence. If the owner of the evidence tries to approve their own evidence, the transaction is declined After approval of created evidence status value changed to 2 as shown in Fig. 6.



```
0: uint8: status 2
1: uint256: eid 1
2: string: data compact disc
3:  address: Owner 0xd3876C6b81408d68D341F4E69e2dE47aBC16
                    Da21
```

FIGURE 6. Output of evidences function after approval by verified super admin.



```
0: uint8: 2
1: string: compact disc
2: address: 0x6fb0d0C9B42f125eC7EC363D6BE38af04f6Bc903
```

FIGURE 7. Output of getEvidenceDetails function after approval of ownership change.

Now if any non-owner user wants to change the ownership of the evidence, then transaction is declined. Only owner of the evidence has the power to change the ownership of the evidence. Then this ownership needs the approval from approved super admin. Now we can use the getEvidenceDetails function to know the details about the evidence. Now we can see the owner of the evidence has been changed as shown in Fig. 7.

Transaction consumes some gas for its execution. This gas consumption can be converted into number of Matic token required for the execution. Then number of Matic token required is multiplied with the Matic token Price in Indian currency. Cost of transaction execution on polygon network for standard execution and rapid execution is shown in Table 1 and 2. Graphical representation of cost analysis for standard execution is shown in Fig. 8

TABLE 1. Cost of transaction execution on polygon network with standard execution.

Gas Price in Matic= .000000138 gwei, Matic Price (INR)= 125				
Sr. No.	**Function**	**Gas Consumed**	**Cost for Standard Execution (Matic)**	**Cost for Standard Execution (INR)**
1	addNewAdmin	50814	0.0070	0.87
2	approveUsers	50708	0.0069	0.86
3	createEvidence	116762	0.0161	2.01
4	changeOwnership	49223	0.0067	0.83
5	approveChangeOwnership	32028	0.0044	0.55

At the time of execution, gas price for rapid execution was 0.000000169 gwei and price of Matic token in INR was 125.

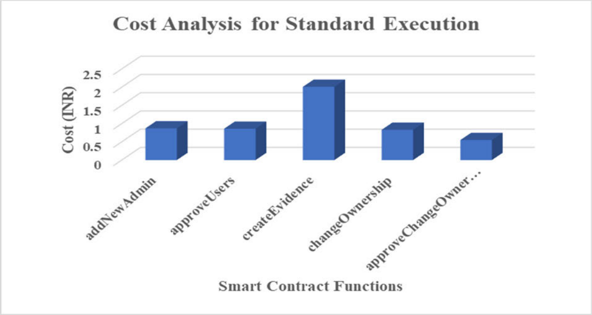


FIGURE 8. Cost analysis for standard execution.

TABLE 2. Cost of transaction execution on polygon network with rapid execution.

Gas Price in Matic= .000000169 gwei, Matic Price (INR)= 125				
Sr.No.	**Function**	**Gas Consumed**	**Cost for Rapid Execution (Matic)**	**Cost for Rapid Execution (INR)**
1	addNewAdmin	50814	0.008588	1.073446
2	approveUsers	50708	0.00857	1.071207
3	createEvidence	116762	0.019733	2.466597
4	changeOwnership	49223	0.008319	1.039836
5	approveChangeOwnership	32028	0.005413	0.676592

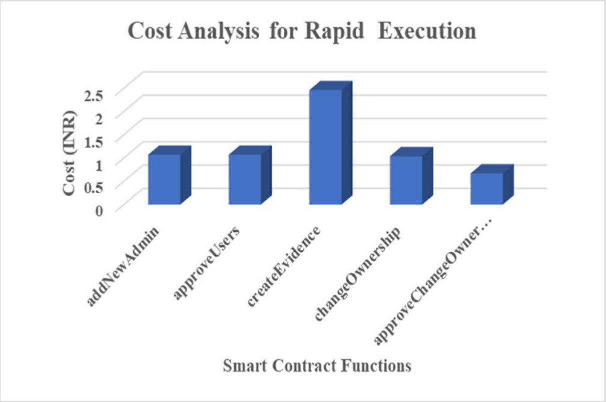


FIGURE 9. Cost analysis for rapid execution.

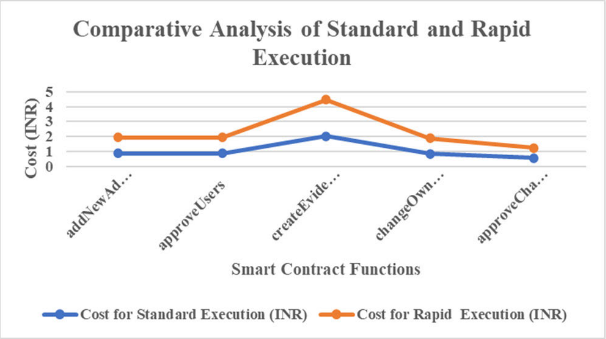


FIGURE 10. Comparative analysis of different functions of smart contract.

These values are considered for the calculation of the function wise cost.

Graphical representation of cost analysis for rapid execution is shown in Fig. 9.

As you can see from Table 1 and 2, the cost of execution is higher with rapid execution as compared to standard execution. The comparative analysis of rapid and standard execution is shown in Fig. 10.

VII. BENEFITS AND LIMITATIONS OF PROPOSED MODEL

A comparison of previous approaches with proposed approach with respect to various parameters such as privacy, authentication, integrity etc. is shown in Table 3.

Proposed model employing blockchain technology in the legal process provides various advantages which are discussed below.

- Evidence sharing without trusted third party: With the proposed model, all evidences can be easily shared with all the entities of the case without involving any third party for the validation of transactions. So, any kind of failure of trust issue can be avoided.
- Retaining evidence integrity: Blockchain technology has a feature of immutability. Because of this feature, if any transaction is written on the ledger, then it cannot be deleted or altered. So, if the information related to evidences once stored on this, nobody can manipulate the information. This is how integrity of the evidences can be retained. This can be very important in current digital world where digital media's reliability is on stake due to fake photos or videos in circulation.
- Digital evidence storage: Maintenance of physical documents overtime is very difficult for example, paper documents go through wear and tear with time, images fade away etc. So, it is better to store these documents in digital form. This can be easily done with the help of proposed model.
- Evidence tracking: All evidences are uploaded on the IPFS and its metadata can be stored on the polygon blockchain. Polygon blockchain will track all the access transactions such who accessed and when etc. from its provenance time to current instance of time.
- Reduction of fraud by increasing transparency: All the accesses to any evidence will be allowed only by the consensus of involved parties and access transactions will be updated in ledgers of all the parties. So, this level of transparency will reduce the chances of fraud or manipulation with the evidences.
- Multi country investigation: There might be some cases where multiple countries need to cooperate to carry out the investigation of any case. In those cases, evidence sharing and maintenance could create problems. With the proposed model, evidence sharing can be easily performed in cross border investigation.

Following are the few threats that can harm the proposed model:

TABLE 3. Comparative analysis of proposed approach with conventional centralized approaches.

Property	1	2	3	4	7	10	14	Proposed Approach
Witness privacy	✓	✓	✓	✓	×	×	×	✓
Juror privacy	×	×	×	×	×	×	×	✓
Authentication	✓	✓	✓	×	✓	✓	✓	✓
Access control	×	×	×	×	✓	×	×	✓
Integrity	✓	✓	✓	✓	✓	✓	✓	✓
Auditability	✓	✓	✓	✓	✓	✓	✓	✓
Traceability	✓	×		×	×		×	✓

- Smart Contract Vulnerabilities: Smart contracts are an integral part of many DApps, and they can be vulnerable to coding errors and security flaws. These vulnerabilities can be exploited to manipulate or steal funds, execute unauthorized transactions, or cause other unintended consequences.
- 51% Attack: In a blockchain network, a 51% attack occurs when a single entity or group of entities gains control of more than 50% of the network's mining power. This allows them to manipulate transactions, block confirmations, and potentially double-spend coins.
- Sybil Attack: A Sybil attack involves creating multiple identities or nodes to gain control over a significant portion of a blockchain network. This allows the attacker to influence the consensus mechanism, disrupt the network, or execute malicious activities.
- Front-End Exploits: DApps often have front-end interfaces, which can be susceptible to traditional web-based attacks such as cross-site scripting (XSS), cross-site request forgery (CSRF), or phishing attacks. These attacks can trick users into revealing their private keys, passwords, or other sensitive information.
- Consensus Protocol Attacks: Blockchain networks rely on consensus mechanisms to validate and agree upon transactions. Depending on the consensus algorithm used (e.g., Proof of Work, Proof of Stake), attacks such as selfish mining, long-range attacks, or stake grinding may be possible, compromising the integrity of the blockchain.
- While IPFS offers decentralized and distributed file storage capabilities, it does have certain considerations related to data availability, reliability, and the potential disappearance of data owners. To address these concerns, it is essential to implement appropriate mitigation strategies and consider additional measures when utilizing IPFS for storing important evidence. Some possible approaches that can help are redundant storage, backups, trusted node operators, data encryption and authentication.

VIII. RESEARCH IMPLICATIONS

In this paper, blockchain technology is used to improve interoperability between the court system and different parties. Our findings can be useful to academicians, researchers, and others in a number of ways. The main use of the findings is to enhance the creation of laws or policies. Second, this research might serve as a starting point for investigations into additional potential applications of blockchain technology in the legal sector. The conclusions offer a thorough understanding of the blockchain-enabled legal system. Researchers will be better able to understand the development and state of blockchain today, which will help them choose worthwhile research topics that demand more devotion from the academic community. More blockchain-based applications may be created for affordable and secure data sharing.

IX. CONCLUSION AND FUTURE WORK

In this paper, we presented a decentralized model for protecting digital evidence using smart contracts on the Layer 2 Polygon blockchain. Our strategy takes advantage of the immutability, transparency, and decentralisation features of blockchain technology to guarantee the security and integrity of digital evidence. We create a trustless, automated system using smart contracts that does away with the need for middlemen and lowers the possibility of tampering or manipulation. We showed that our decentralised model is effective and efficient through our experimental evaluation. Real-world applications can benefit from the deployment of the Layer 2 Polygon blockchain because it enables scalable and affordable storage and verification of digital evidence. We make sure the evidence is intact and verifiable throughout its lifecycle by utilising the security characteristics of smart contracts. There are still a few areas, though, that need improvement and more research. The scalability of blockchain technology is one of the major issues since the amount of storage needed for digital proof can soon rise to a significant level. For vast volumes of evidence to be handled effectively in the future, storage and retrieval procedures should be optimised. The incorporation of cutting-edge cryptographic methods to improve the confidentiality and privacy of digital evidence represents another area for future study.

Techniques such as zero-knowledge proofs or homomorphic encryption can be explored to enable secure computations on encrypted evidence without revealing sensitive information. Furthermore, the usability and accessibility of the system should be improved to encourage widespread adoption. User-friendly interfaces and seamless integration with existing digital forensic tools can help bridge the gap between traditional forensic workflows and decentralized systems. Lastly, the legal and regulatory aspects surrounding the use of decentralized systems for handling digital evidence need to be addressed. Collaboration with legal experts and policymakers is crucial to ensure compliance with existing laws and regulations and to establish a legal framework that accommodates the unique features and challenges of decentralized systems.

CONFLICT OF INTEREST

No Conflict of Interest.

REFERENCES

[1] A. Nieto, R. Roman, and J. Lopez, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," *IEEE Netw.*, vol. 30, no. 6, pp. 34–41, Nov. 2016.

[2] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.

[3] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Inf. Sci.*, vol. 491, pp. 151–165, Jul. 2019.

[4] X. Lin, T. Chen, T. Zhu, K. Yang, and F. Wei, "Automated forensic analysis of mobile applications on Android devices," *Digit. Invest.*, vol. 26, pp. S59–S66, Jul. 2018.

[5] A. Shafarenko, "A PLS blockchain for IoT applications: Protocols and architecture," *Cybersecurity*, vol. 4, no. 1, pp. 1–17, Feb. 2021.

[6] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[7] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[8] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-IoT using blockchain technology," *IEEE Access*, vol. 7, pp. 99573–99588, 2019.

[9] S. Ghimire, J. Y. Choi, and B. Lee, "Using blockchain for improved video integrity verification," *IEEE Trans. Multimedia*, vol. 22, no. 1, pp. 108–121, Jan. 2020.

[10] M. Pourvahab and G. Ekbatanifard, "Digital forensics architecture for evidence collection and provenance preservation in IaaS cloud environment using SDN and blockchain technology," *IEEE Access*, vol. 7, pp. 153349–153364, 2019.

[11] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, "LedgerDB: A centralized ledger database for universal audit and verification," *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, Aug. 2020.

[12] J. Sun, X. Yao, S. Wang, and Y. Wu, "Non-repudiation storage and access control scheme of insurance data based on blockchain in IPFS," *IEEE Access*, vol. 8, pp. 155145–155155, 2020.

[13] S. Li, T. Qin, and G. Min, "Blockchain-based digital forensics investigation framework in the Internet of Things and social systems," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1433–1441, Dec. 2019.

[14] M. Lusetti, L. Salsi, and A. Dallatana, "A blockchain based solution for the custody of digital files in forensic medicine," *Forensic Sci. Int., Digit. Invest.*, vol. 35, Dec. 2020, Art. no. 301017.

[15] B. C. A. Petroni, R. F. Gonçalves, P. Sérgio de Arruda Ignácio, J. Z. Reis, and G. J. D. U. Martins, "Smart contracts applied to a functional architecture for storage and maintenance of digital chain of custody using blockchain," *Forensic Sci. Int., Digit. Invest.*, vol. 34, Sep. 2020, Art. no. 300985.

[16] D. Ramesh, R. Mishra, P. K. Atrey, D. R. Edla, S. Misra, and L. Qi, "Blockchain based efficient tamper-proof EHR storage for decentralized cloud-assisted storage," *Alexandria Eng. J.*, vol. 68, pp. 205–226, Apr. 2023.

[17] 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. Invest.*, vol. 33, Jun. 2020, Art. no. 300976.

[18] G. Gürsoy, C. M. Brannon, and M. Gerstein, "Using Ethereum blockchain to store and query pharmacogenomics data via smart contracts," *BMC Med. Genomics*, vol. 13, no. 1, pp. 1–11, Jun. 2020.

[19] M. Li, C. Lal, M. Conti, and D. Hu, "LEChain: A blockchain-based lawful evidence management scheme for digital forensics," *Future Gener. Comput. Syst.*, vol. 115, pp. 406–420, Feb. 2021.

[20] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[21] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 1–36, 2014.

[22] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[23] R. Stoykova, "The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations," *Comput. Law Secur. Rev.*, vol. 49, Jul. 2023, Art. no. 105801.

[24] R. S. Pereira, "Evidence models and proof of causation," *Law, Probab. Risk*, vol. 12, nos. 3–4, pp. 229–257, Sep. 2013.

[25] S. K. Rana, S. K. Rana, A. K. Rana, K. Nisar, T. R. Soomro, and S. Nisar, "A survey on blockchain technology supported approaches for healthcare system, open issues and challenges," in *Proc. 14th Int. Conf. Math., Actuarial Sci., Comput. Sci. Statist. (MACS)*, Nov. 2022, pp. 1–7.

[26] S. K. Rana, S. K. Rana, A. K. Rana, and S. M. N. Islam, "A blockchain supported model for secure exchange of land ownership: An innovative approach," in *Proc. Int. Conf. Comput., Commun., Intell. Syst. (ICCCIS)*, Nov. 2022, pp. 484–489.

[27] S. K. Rana and S. K. Rana, "Blockchain based business model for digital assets management in trust less collaborative environment," *J. Crit. Rev.*, vol. 7, no. 9, pp. 738–750, Jul. 2020.

[28] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, Apr. 2021.

[29] D. Dias and J. Benet, "Distributed Web Applications with IPFS," in *Proc. Int. Conf. Web Eng.*, Lugano, Switzerland, 2016, pp. 616–619.

[30] P. Santamaría, L. Tobarra, R. Pastor-Vargas, and A. Robles-Gómez, "Smart contracts for managing the chain-of-custody of digital evidence: A practical case of study," *Smart Cities*, vol. 6, no. 2, pp. 709–727, Feb. 2023.

[31] M. N. A. Khan and S. Ullah, "A log aggregation forensic analysis framework for cloud computing environments," *Comput. Fraud Secur.*, vol. 2017, no. 7, pp. 11–16, Jul. 2017.

[32] P. M. Trenwith and H. S. Venter, "FReadyPass: A digital forensic ready passport to control access to data across jurisdictional boundaries," *Austral. J. Forensic Sci.*, vol. 51, no. 5, pp. 583–595, Sep. 2019.

[33] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "A forensic acquisition and analysis system for IaaS," *Cluster Comput.*, vol. 19, no. 1, pp. 439–453, Mar. 2016.

[34] S. K. Rana and S. K. Rana, "Intelligent amalgamation of blockchain technology with industry 4.0 to improve security," in *Internet of Things*, 1st ed. London, U.K.: CRC Press, 2021, pp. 165–175, ch. 12.

[35] M. Irfan, H. Abbas, Y. Sun, A. Sajid, and M. Pasha, "A framework for cloud forensics evidence collection and analysis using security information and event management," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3790–3807, Jul. 2016.

[36] D. Spiekermann, J. Keller, and T. Eggendorfer, "Network forensic investigation in OpenFlow networks with ForCon," *Digit. Invest.*, vol. 20, pp. S66–S74, Mar. 2017.

[37] P. Santra, R. Prasanna, H. Debojyoti, and M. Puspa, "Fuzzy data mining-based framework for forensic analysis and evidence generation in cloud environment," in *Ambient Communications and Computer Systems*. Singapore: Springer, 2018, pp. 119–129.

[38] L. Pasquale, S. Hanvey, M. Mcgloin, and B. Nuseibeh, "Adaptive evidence collection in the cloud using attack scenarios," *Comput. Secur.*, vol. 59, pp. 236–254, Jun. 2016.

[39] R. Norvill, B. B. Fiz Pontiveros, R. State, and A. Cullen, "IPFS for reduction of chain size in Ethereum," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1121–1128.

SUMIT KUMAR RANA received the B.Tech. degree from Kurukshetra University, and the M.Tech. and Ph.D. degrees from Maharishi Markandeshwar (Deemed to be University), Mullana, India. He is currently an Assistant Professor with the Panipat Institute of Engineering and Technology, Panipat, India, with more than 12 years of experience. He is a collaborative researcher. Also, he has attended various workshops and faculty development programs. He has guided four M.Tech. candidates. He has a keen interest in teaching and implementing the latest techniques related to blockchain technology. He has published multiple SCI/SCOPUS articles, book chapters, and papers in national and international IEEE conferences. He also published national patent. His research interests include blockchain technology, cryptography, cryptocurrency, and artificial intelligence. He is a member of the Computer Science Teachers Association (CSTA) and the International Association of Engineers (IAENG). He serves as a reviewer for several journals and international conferences.

ARUN KUMAR RANA received the B.Tech. degree from Kurukshetra University, and the M.Tech. and Ph.D. degrees from Maharishi Markandeshwar (Deemed to be University), Mullana, India. He is currently an Assistant Professor-3 with the Galgotias College of Engineering and Technology, Greater Noida, India, with more than 16 years of experience. He is a collaborative researcher. He has published more than 120 SCI/ESCI/Scopus/others articles in national and international journals and also in conferences. He has also published ten books with a national and international publisher, such as Taylor and Francis, USA. He was a member of SCI and Scopus-indexed international conference/symposium for many times. He has guided six M.Tech. candidates. He has published/granted ten national and international patents. His research interests include image processing, wireless sensor networks, the Internet of Things, AI, machine learning, and embedded systems. He is a member of the Asia Society of Research and the Scientific Innovation Research Group (SIRG), Egypt. He is an editor and a reviewer of many international journals around the world. He serves as a reviewer for several journals and international conferences. He was a keynote speaker in international conference for many time. He has conducted many workshops on the IoT and its applications in engineering and wireless networks and simulators. He received international awards from the various international organization (many times). He was listed in the world scientist ranking, in 2021 and 2022. He was a Guest Editor of Special Issue ‘‘Routing and Protocols for Energy Efficient Communication’’ Energy, MDPI, SCI, IF-3.004 (Q2); Special Issue in Blockchain in Industry, Frontier Publication (ESCI Indexed, IF:2.252). Q2 Cat. Journal; Special Issue in *Journal of Autonomous*, Frontier Publication (Scopus-Indexed, IF:3.252). Q2 Cat. Journal.

SANJEEV KUMAR RANA received the B.Tech. degree in computer engineering from Kurukshetra University, Kurukshetra, India, in 1999, the M.Tech. degree in information technology from GGSIP University, in 2007, and the Ph.D. degree from the Department of Computer Science and Engineering, Maharishi Markandeshwar (Deemed to be University), Mullana, India, in 2012. He has published more than 60 papers in MANETs, blockchain technology, cryptography and network security, computer networks, and mobile computing in international conferences and international journals/SCI/Scopus. His research interests include wireless networks, big data, and blockchain technology.

VISHNU SHARMA (Member, IEEE) received the B.Tech. degree in computer science and engineering from the Government Autonomous Institute, the M.Tech. degree in computer science and engineering from the Madhav Institute of Technology and Science (MITS), Gwalior, Madhya Pradesh, and the Ph.D. degree in computer science and engineering from Rajiv Gandhi Technical University, Bhopal, in 2012. He is a Professor and the Head of the CSE Department, Galgotias College of Engineering and Technology, Greater Noida, Uttar Pradesh. He is having around 21 years of teaching experience in various reputed engineering institutes and universities, such as Jaypee University, Galgotias University, KIET, and Galgotias College. He has published more than 60 papers in MANETs, AI, machine learning, the IoT, cryptography and network security, computer networks, and mobile computing in international conferences and international journals/SCI/Scopus. He has published three books on mobile computing, fundamental of cyber security and law, and advanced mobile computing. He has also organized many IEEE international conferences in the IEEE UP section. He is a Guest Editor of special issue in Blockchain in Industry, Frontier Publication (ESCI Indexed, IF:2.252). Q2 Cat. Journal.

UMESH KUMAR LILHORE received the Doctoral and Postdoctoral degrees in CSE. He is a Professor with the Department of CSE, Chandigarh University, Punjab, India. He has more than 17 years of experience in teaching, research, and industry. He has research publications in SCI-indexed international journals of high repute. His research interests include AI, machine learning, computer security, computational intelligence, and information science.

OSAMAH IBRAHIM KHALAF received the B.Sc. degree in software engineering from Al-Rafidain University College, Iraq, in 2004, the M.Sc. degree in computer engineering from Belarussian National Technical University, in 2007, and the Ph.D. degree in computer networks from the Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, in 2017. He is a Senior Engineering and a Telecommunications Lecturer with Al-Nahrain University. He has 15 years of university-level teaching experience in computer science and network technology and a strong CV about research activities in computer science and information technology projects. He has overseas work experiences with University in Binary, University in Malaysia, and University Malaysia Pahang. He has many published articles indexed in ISI/Thomson Reuters. He has also participated and presented at numerous international conferences. He has a patent and received several medals and awards due to his innovative work and research activities. He has good skills in software engineering, including experience with .Net, SQL development, database management, mobile applications design, mobile techniques, Java development, android development, IOS mobile development, cloud system and computations, and website design.

ANTONINO GALLETTA (Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in computer engineering from The University of Messina, and the Ph.D. degree from the University of Reggio Calabria, Italy.

He is an Assistant Professor with The University of Messina. Before starting the Ph.D., he was a Senior Software Developer and a Team Leader with The University of Messina, from 2013 to 2016. Currently, he is the PI of ‘‘InstradaME’’ an Italian Project funded by the Ministry of Interior. In 2019, he was the PI of Helsinki Noise and Air quality Monitoring systEm (NAME), a project funded by the European Pre-Commercial Procurement Project ‘‘Select for Cities.’’ His main research activities focus on the security of cloud/edge/IoT technologies for smart cities and e-health solutions, including big data management and blockchain.

Open Access funding provided by ‘Università degli Studi di Messina’ within the CRUI CARE Agreement