Chapter 10
Robust and Secure Evidence Management in Digital Forensics Investigations Using Blockchain Technology

Sajidha S. A
https://orcid.org/0000-0003-4771-3131
Vellore Institute of Technology, Chennai, India

Rishik Kumar
Vellore Institute of Technology, Chennai, India

Lavanya Puri
Vellore Institute of Technology, Chennai, India

Manya Gaur
Vellore Institute of Technology, Chennai, India

Shreya Manoj Kumar
Vellore Institute of Technology, Chennai, India

Amit Kumar Tyagi
https://orcid.org/0000-0003-2657-8700
National Institute of Fashion Technology, Delhi, India

Jahangeer Sidiq S
Vellore Institute of Technology, Chennai, India

Nisha V. M.
Vellore Institute of Technology, Chennai, India

ABSTRACT

The chapter proposes a framework for evidence management in digital forensic investigations that leverages blockchain technology to ensure integrity and authenticity of the chain of custody process. The framework utilizes smart contracts, nodes, and consensus algorithms to create a tamper-proof record of the entire chain of custody process from evidence collection to presentation. A contract that facilitates transfer of ownership of the forensic report from the forensic laboratory to the

DOI: 10.4018/978-1-6684-8938-3.ch010

investigation department is implemented. Using this approach, the authors ensure integrity and security of the forensic report, thereby mitigating any potential risks of tampering or compromise through unethical means. A robust framework to safeguard credibility of forensic report to maintain the chain of custody, instilling confidence in the reliability of the investigative process is established. Traditional methods of evidence management, showing that the proposed framework offers a secure, reliable, and transparent solution for managing digital evidence in digital forensics investigations has been proved.

INTRODUCTION

This paper is specifically directed towards individuals engaged in the field of forensic studies, with a particular emphasis on digital forensic analysts. Additionally, it extends its relevance to cybersecurity professionals actively involved in forensic investigations. Given the expanding footprint of blockchain technology within the healthcare sector, this research work serves as a pivotal stepping stone towards the integration of blockchain solutions into the realm of digital forensics. By addressing the synergies and potential applications of blockchain in this context, this paper paves the way for the establishment of a robust foundation for the utilization of blockchain technology in the enhancement of digital forensic practices.

In recent times, there is a growing trend towards the digitalization of forensic reports[5], mirroring the progression observed in the digitalization of Health Records, commonly known as Electronic Health Records (EHR) or Electronic Medical Reports (EMR). Forensic reports hold critical information pertaining to crime scenes, evidence collection, laboratory analysis, and expert opinions. The utilization of digital evidence plays a pivotal role in digital forensics investigations. However, conventional methods of evidence management have exhibited vulnerabilities to human errors, tampering, and fraudulent activities, consequently posing challenges on reliability and integrity of the evidence.

To overcome these challenges, blockchain technology has emerged as a promising solution for the management of digital evidence. It offers a distributed ledger system that can establish a tamper-proof and decentralized platform for the storage and management of data[1].

Blockchain technology initially emerged as a distributed database solution to keep a decentralized log of transactions performed. The primary idea behind securing the transaction log is to distribute the data among different nodes connected in a chain where changing or modifying each node unethically requires computational power[3]. The reason for the high security and integrity of blockchain is because of various methods such as ‘proof of work’. Modifying data unethically requires the same type of modification across all blocks in a distributed network that would require tremendous amount of computational power. Because of its high reliability for storing data, blockchain soon began to be implemented in other areas too.

The paper does not cover the basics or the fundamentals of blockchain technology although certain terminologies that have been used throughout the chapter related to blockchain have been discussed briefly. It would still be recommended that the reader familiarizes themselves with the fundamentals of blockchain technology before proceeding to read the rest of the chapter. The references cite the sources that deal with security of blockchain technology and its vulnerabilities as well as applications and scope of blockchain in healthcare and forensics, although it does not cite any sources that deal with the basic concepts of blockchain.

The paper makes reference to the use of solidity as well as truffle framework which is used for developing private blockchain networks.

By leveraging blockchain technology, forensic practitioners can enhance the trustworthiness, transparency, and security of forensic reports[7]. The decentralized nature of blockchain eliminates the need for a centralized authority, reducing the risk of unauthorized access, manipulation, or loss of critical evidence. Each transaction or modification made to the digital evidence is recorded on the blockchain, creating an indelible record of its journey, from collection to analysis, ensuring an auditable and transparent process.

The immutability of blockchain ensures that once data is recorded, it cannot be altered without leaving a trace, establishing a strong foundation for maintaining the chain of custody.

Additionally, blockchain technology enables efficient collaboration and information sharing among multiple stakeholders[4] involved in the forensic investigation process. Authorized participants, such as forensic experts, law enforcement agencies, and legal professionals, can securely access and validate the evidence stored on the blockchain, facilitating seamless collaboration, and reducing the potential for disputes or discrepancies.

Overall, the adoption of blockchain technology in managing digital evidence has the potential to revolutionize the field of digital forensics, improving the reliability, transparency, and security of forensic reports. By leveraging the decentralized and tamper-proof nature of blockchain, forensic practitioners can enhance the trustworthiness of digital evidence and strengthen the credibility of their investigative findings, ultimately contributing to more robust and effective legal proceedings.

To this end, this research paper proposes a blockchain-based digital forensics chain of custody framework. This framework utilizes smart contracts, nodes, and consensus algorithms to create a tamper-proof record of the entire chain of custody process, from evidence collection to presentation. The proposed framework provides a transparent and decentralized platform that ensures the reliability and integrity of digital evidence management.

The framework offers several security features that enhance the integrity of the chain of custody process. For example, it offers a tamper-proof record of all transactions, which is distributed across the network and cannot be altered without consensus. Additionally, the framework offers an audit trail that can be used to track the history of evidence, as well as the identities of all parties involved in the chain of custody process.

In comparison to traditional methods of evidence management, the proposed blockchain-based framework offers several advantages. These include enhanced security, transparency[6], and reliability, which can be critical in digital forensics investigations. AI based assistive health care[4] systems can also use the proposed system and provide more secure, transparent services to the user and the other end users.

RELATED WORKS

Various assistive technologies use health care reports and personal details which could be easily shared across home, across county or state boundaries. Block chain has made travelling life easier by providing secure, personalized health care. Thus, avoiding the need to recurrently communicate the similar information to a many naïve users who provide services for the wide range of facilities and resources.

Blockchain-based digital forensics chain of custody is a developing area of study that seeks to offer a tamper-proof and transparent record of the chain of custody in digital forensics investigations. Although the body of literature on this subject is still in its infancy, some prominent studies have examined the application of blockchain technology in this context.

Mamun Ahmed et al.[1] focus on creating a blockchain based medical forensic system by utilizing hyperledger. The work focuses on tracing any access or modification which has not been authorized, and makes an attempt towards ensuring that secrecy and integrity of the data is secured.

Chin-Ling Chen et al.[5] propose a model that can verify the correctness and integrity of a protocol within the domain of digital healthcare communications. The work emphasizes on integrating the system with blockchain technology and discusses the requisites for implementing this system. The work also focuses on some cryptography techniques for ensuring safety of data.

Auqib Hamid et al.[10] discusses the forensic investigation of chain of custody and proposes a model for keeping track of all changes and recording logs for a better security and transparency. They propose a five component forensic chain architecture and discuss its advantages and limitations while considering the current problems at hand.

Zhang Wenhua et al.[13] in their work, highlight the different types of security issues and vulnerabilities correlating to various consensus mechanisms, limitations of different consensus algorithms, how to handle the vulnerabilities exisitng in different networks, and the future scope and applications of such blockchain systems in the field of healthcare.

Sharing of data and the fear of compromising of privacy among patients has been a major hurdle in promotion of Electronic Medical Reports. Qianqian Su et al.[12] focus on this problem by introducing a scheme within their system which takes a unique signature as an attribute from the patients to assure who has the access to the patient's data. Their work focuses on implementing this system by using KUNodes algorithm and evaluating the feasibility of such a system.

Peng Xi et al.[14] focus on surveying different blockchain technologies available for storing patient data for digital healthcare communication systems and to maintain the integrity of the system as well as privacy of data. The work discusses applications of digital healthcare communication systems and different scenarios where sharing of patients' data might be needed and gives an in depth analysis for the same.

Amaal Zakzouk et al.[15] discuss the privacy issues, security loopholes and vulnerabilities in digital healthcare systems and propose blockchain based electronic medical report framework for management of health records and healthcare communications. The work further discusses the scalability aspects of such system and challenges faced in maintaining the integrity of the system and the medical records.

However, there are a few ways by which our proposed work stands out:

Performance: Proposed work's chain of custody mechanism can handle a larger volume of digital evidence faster and more accurately than existing solutions; it could be considered better than others.

Table 1. Comparison table for papers

Paper Number	Blockchain Technology Used	Key Findings
1	Private blockchain	Proposed a blockchain-based solution for the chain of custody in digital forensics using a private blockchain.
2	Public and private blockchains	Provided an overview of the use of blockchain technology in digital forensics and highlighted the potential advantages and challenges of using public and private blockchains.
3	Public and private blockchains	Explored the potential of blockchain technology in digital forensics investigations and highlighted the need for further research in this area.
4	N/A	Provided an overview of the chain of custody in digital forensics investigations and highlighted the challenges associated with preserving it.
5	Public and private blockchains	Provided an overview of the use of blockchain technology in digital forensics and discussed the potential advantages and challenges of using public and private blockchains.
6	Public blockchain	Proposed a blockchain-based solution for the chain of custody in digital forensics using a public blockchain.
7	Private blockchain	Proposed a blockchain-based solution for the chain of custody in digital forensics using a private blockchain.
8	Public blockchain	Proposed a blockchain-based solution for the chain of custody in supply chain management to prevent counterfeiting using a public blockchain.
9	Private blockchain	Provided an overview of the use of blockchain technology in digital forensics investigations and discussed the potential advantages and challenges of using private blockchain..
10	Private blockchain	Proposed a blockchain-based solution for evidence management in digital forensics investigations using a private blockchain.
11	Public blockchain	Proposed a blockchain-based solution for the chain of custody in supply chain management to prevent counterfeiting using a public blockchain.

Usability: We can provide an easy-to-use interface for investigators and other stakeholders to access and manage digital evidence, it could be considered better than others.

Security: Its blockchain-based solution can provide a higher level of security and protection for digital evidence than existing solutions by the use of hash keys.

Scalability: The proposed work can also demonstrate scalability to handle an increasing number of digital evidence, it could be considered better than others.

We have provided a comprehensive overview of recent papers that focus on the application of blockchain technology in the domains of medical healthcare and forensics (**Table 1**).

METHODOLOGY

We use Hard Hat to deploy a local blockchain network, the network will solely be used for different forensic labs. Each forensic lab will have a unique address. Similarly each forensic expert and each subject will have a unique ID. Each of these IDs will be mapped to the relevant forensic expert ID and forensic lab address. Only the forensic expert will have access to enter a new record in the blockchain network.

Any entry from any other address will be rejected and the attempted modifications will be nullified. As soon as a

new entry is made, the system shall automatically map the latest entry to the correct unique IDs.

The smart contract will be deployed on a private blockchain network and its Application Binary Interface address(ABI Address) will be used to display the details on a client side front-end. Again this access will be only available to certain unique IDs. This way we make sure there is no illegal compromising of forensic reports.

Architecture

The architecture for blockchain for digital forensics using Solidity and Truffle can be divided into several components:

1. Blockchain Network: This is the underlying infrastructure that enables the storage of data in a decentralized, tamper-proof manner. The blockchain network serves as the fundamental infrastructure that facilitates the decentralized and tamper-proof storage of data. It provides the underlying framework for implementing a secure and transparent system for various applications, including the management of digital evidence in the field of forensic investigations. In the proposed architecture, Ethereum has been chosen as the blockchain network of choice.

Ethereum is a well-known and widely used blockchain platform. It offers a range of features and functionalities that make it suitable for our purposes. It is a decentralized, open-source blockchain network that supports the execution of smart contracts. These smart contracts are self-executing agreements with predefined rules and conditions, allowing for the automation and enforcement of various processes.

By utilizing Ethereum as the blockchain network, we can leverage its robust infrastructure and ecosystem. Ethereum's consensus mechanism[2], known as Proof-of-Work (PoW) or Proof-of-Stake (PoS), ensures the security and integrity of the network. It relies on a distributed network of nodes that collectively validate transactions and maintain the blockchain ledger. Ethereum provides a high level of transparency. All transactions and modifications made to the blockchain are recorded in a public ledger, allowing for easy auditing and verification. This transparency ensures that the integrity of the digital evidence stored within the blockchain can be easily verified by authorized stakeholders, such as forensic experts, law enforcement agencies, and legal professionals.

2. Smart contracts play a pivotal role in our proposed framework, as they enable the automation and enforcement of rules and processes in a secure and transparent manner. These self-executing contracts are designed to incorporate the terms and conditions of an agreement directly into lines of code, eliminating the need for intermediaries and ensuring the integrity and trustworthiness of the contract execution. In the context of digital forensics, smart contracts offer valuable capabilities for managing and securing digital evidence.

By leveraging smart contracts, we establish a systematic and reliable approach to enforce rules and automate key processes in the management of digital evidence. The use of smart contracts allows us to define and execute predefined actions based on specific events or conditions, ensuring consistency and reducing the potential for human error or manipulation. This automation streamlines the chain of custody process, minimizing manual intervention and enhancing the overall efficiency of forensic investigations.

To create these smart contracts, we will be utilizing the Solidity programming language. Solidity is specifically designed for developing smart contracts on the Ethereum blockchain network, making it an ideal choice for our framework. Solidity offers a range of features and syntax that enable the implementation of complex business logic and rules within smart contracts. With Solidity, we can define the behavior and functionalities of the smart contracts, including the validation of digital evidence, the recording of key events, and the enforcement of rules related to evidence handling and access control. The programming language provides mechanisms for data storage, contract interaction, and event handling, enabling seamless integration with the overall blockchain-based system.

3. Truffle is a comprehensive development environment, testing framework, and asset pipeline specifically designed for Ethereum-based projects. It offers a suite of tools that facilitate the seamless development, testing, and deployment of smart contracts on the Ethereum blockchain. Truffle's features and functionalities greatly enhance the efficiency and reliability of the smart contract development process.

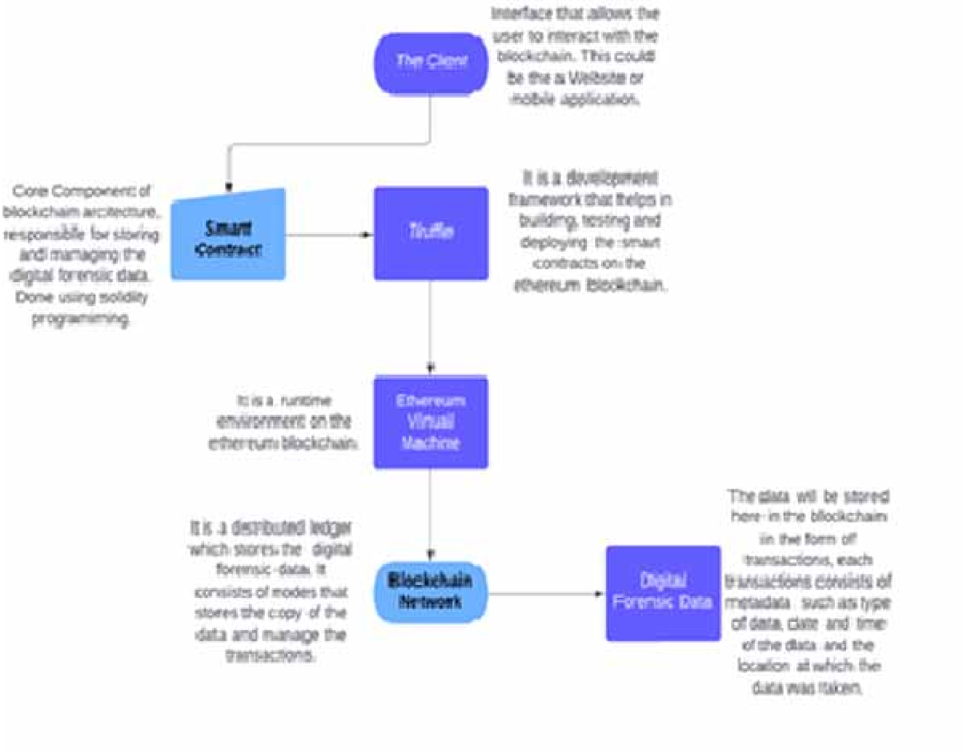
As a development environment, Truffle provides a user-friendly interface and a range of utilities that simplify the creation of Ethereum-based applications. It offers a standardized project structure, making it easier to organize and manage smart contract code, configuration files, and other project assets. Truffle also includes a built-in development server that allows developers to interact with their smart contracts locally during the development phase.

Truffle also includes a powerful asset pipeline that streamlines the process of managing project assets such as JavaScript, CSS, and HTML files. This asset pipeline automates the compilation, optimization, and deployment of these assets, ensuring that they are seamlessly integrated with the smart contract deployment process. This simplifies the overall project management and deployment workflow.

4. Web3.js is a powerful JavaScript library that enables developers to interact with the Ethereum blockchain and build web applications that interact with smart contracts. It provides a comprehensive set of Application Programming Interfaces (APIs) that facilitate seamless integration with the Ethereum network and enable the execution of various blockchain-related functionalities. The library offers a range of functions and methods that allow developers to connect to the blockchain, send transactions, query data, and interact with smart contracts Developers can utilize the library to instantiate smart contract instances, access contract methods, and retrieve contract data. The retrieval of data is one of the crucial points for opting web3.js as it facilitates in accessing the data that is existent in the blockchain network in a secure manner.

Furthermore, Web3.js supports event handling, which is essential for monitoring and reacting to events emitted by smart contracts.

Figure 1. Architecture flow: Depicting the architecture of the proposed methodology


Interface that allows the user to interact with the blockchain. This could be the a Website or mobile application.
The Client
Core Component of blockchain arcitecture, responsible for storing and managing the digital forensic data. Done using solidity programming.
Smart Contract
Truffle
It is a development framework that helps in building, testing and deploying the smart contracts on the ethereum Blockchain.
It is a runtime environment on the ethereum blockchain.
Ethereum Virtual Machine
It is a distributed ledger which stores the digital forensic data. It consists of modes that stores the copy of the data and manage the transactions.
Blockchain Network
Digital Forensic Data
The data will be stored here in the blockchain in the form of transactions, each transactions consists of metadata such as type of data, date and time of the data and the location at which the data was taken.

Developers can define event listeners that capture and respond to specific events emitted by smart contracts. This enables real-time updates and notifications within web applications, providing a dynamic and interactive user experience. This makes it suitable for our prototype for the future scope of development and other future inspired works. Its extensive set of APIs simplifies account management, transaction signing, smart contract interaction, event handling.

The smart contract helps to interact with the blockchain network where the data is secured as depicted through the architecture of the proposed methodology **(Figure 1)**. The Figure 1 provides a comprehensive visual representation of the components and their interactions within the system.

Solidity and Truffle

1. Create Smart Contracts: The initial phase of our approach involves the creation of smart contracts that serve as the foundation for managing digital forensics processes. These smart contracts, written in Solidity, a programming

language specifically designed for Ethereum, will be deployed on the Ethereum blockchain, providing a secure and decentralized platform for executing the defined rules and processes. We will leverage the capabilities of Solidity to implement the rules and processes that govern digital forensics investigations, ensuring transparency, reliability, and immutability throughout the process.

2. Compile Smart Contracts: By compiling the smart contracts, we generate bytecode, which consists of a series of instructions that define the behavior and functionality of the contracts. This bytecode is then ready to be deployed onto the Ethereum blockchain, where it will be executed by the Ethereum Virtual Machine. The bytecode generated during the compilation process is specific to the Ethereum blockchain and can only be executed within the Ethereum ecosystem. This bytecode is not executable on other blockchain platforms or traditional computing environments.
3. Deploy Smart Contracts: Once the smart contracts are developed, they will be deployed on the Ethereum blockchain. Through the deployment of smart contracts on the Ethereum blockchain, we establish a reliable and immutable framework for digital forensics. The transparency and traceability offered by the blockchain enable all stakeholders to verify and validate the processes and actions recorded in the smart contracts. This fosters trust and enhances the credibility of digital forensic investigations. To facilitate this process, we utilize Truffle, a development environment, testing framework, and asset pipeline specifically designed for Ethereum.

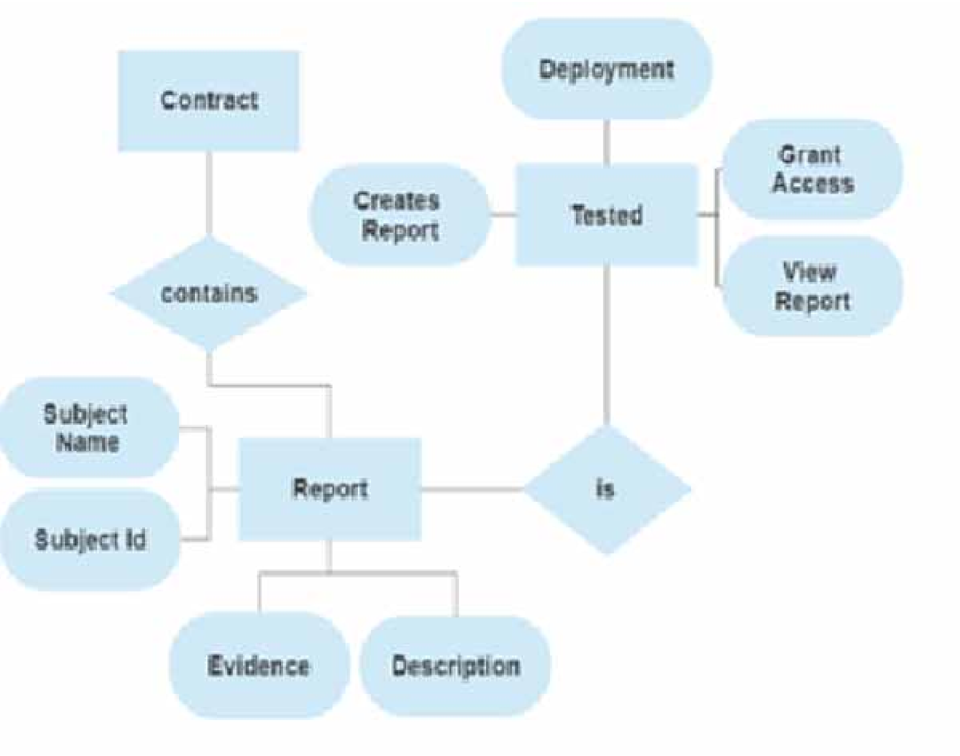
Truffle provides a comprehensive suite of tools that streamline the deployment of smart contracts onto the Ethereum blockchain. These tools simplify the configuration, management, and deployment of smart contracts, making the process more efficient and developer-friendly. Truffle allows developers to define deployment scripts that specify the contracts to be deployed, their constructor arguments, and any additional deployment configurations. These scripts provide a structured and reproducible approach to deploying smart contracts.

4. Interact with Smart Contracts: Once the smart contracts are deployed, they can be interacted with using Web3.js. This allows developers to build web applications that can interact with the smart contracts.
5. Test Smart Contracts: Truffle provides a testing framework that can be used to write tests for smart contracts. This ensures that the contracts are working as intended and that there are no bugs.
6. Debug Smart Contracts: Truffle also provides a debugging tool that can be used to debug smart contracts. This is useful for identifying and fixing bugs in the contracts.

7. Monitor Smart Contracts: Once the smart contracts are deployed on the Ethereum blockchain, it is crucial to monitor their performance and functionality to ensure they are operating as intended. Monitoring smart contracts helps detect any unexpected behavior, identify potential issues or vulnerabilities, and ensure the overall health and reliability of the system. Fortunately, there are several monitoring tools available specifically designed for Ethereum-based smart contracts.

Truffle Debugger is an integrated development environment (IDE) that offers debugging capabilities for Ethereum smart contracts. It allows developers to step through the contract code, inspect variable values, and analyze the contract's execution flow. Truffle Debugger is particularly useful during the development and testing phases to identify and resolve any issues in the contract logic. Another popular monitoring tool is Etherscan. Etherscan is a web-based platform that provides real-time monitoring and analysis of Ethereum-based transactions, smart contracts, and addresses.

Figure 2. Entity relationship diagram



Overall, the architecture for blockchain for digital forensics using Solidity and Truffle provides a secure, decentralized, and tamper-proof method for storing and processing digital forensics data.

Entity relationship diagram shows the relationship between back-end components and working procedure **(Figure 2)**.

Smart Contract

A smart contract is a self-executing digital agreement that is built on a blockchain platform, such as Ethereum. It is a computer program that automatically enforces the terms and conditions of the agreement, eliminating the need for intermediaries and providing transparency, security, and efficiency. Smart contracts facilitate and verify the negotiation and performance of contracts without relying on centralized authorities, enabling parties to interact and exchange assets in a trustless manner, while also reducing costs and minimizing the potential for fraud.

In a smart contract, rules are the predefined conditions and logic that govern the behavior and execution of the contract. These rules are encoded into the contract's code and dictate how the contract should operate and respond to different inputs or events. They define the rights, obligations, and actions of the parties involved in the contract. For example, rules can include conditions for triggering specific actions or payments, validating input data, enforcing deadlines, or defining dispute resolution mechanisms. Smart contract rules are transparent, immutable, and automatically executed, ensuring that all parties adhere to the agreed-upon terms without the need for intermediaries or manual intervention.

For our proposed methodology, we utilize the following components in order to implement the forensic report safely and securely:

1. Contract Structure

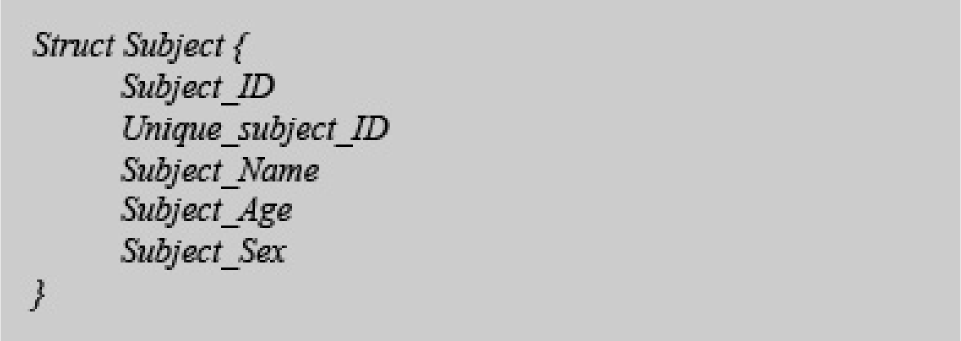
Figure 3. Contract structure

```
Contract ForensicReport{
...
}
```

The contract encompasses the all the defined the variables, functions, and other logic that make up the behavior of the contract dictate how the contract will execute without any central authority **(Figure 3.)**.

2. Subject

Figure 4. Subject

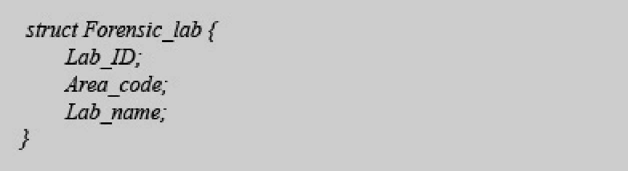


```
Struct Subject {
        Subject_ID
        Unique_subject_ID
        Subject_Name
        Subject_Age
        Subject_Sex
}
```

'Subject' is a custom data structure which holds details of a subject. The subject here refers to person on which forensic tests are done. The structure holds the entities 'subject_ID' which is a unique ID given to each subject **(Figure 4.)**. 'Unique_subject_ID' refers to another unique ID which is generated by the hash function of our code. This is generated by taking into account all the properties of the Subject including 'Subject_ID'. This way, any third party who wants to gain access to the forensic report information must have access to the subject_ID as well as Unique_subject_ID. For the sake of simplicity, we used Keccak-256 algorithm for hashing but the hashing function can be modified based on the level of security need. Other attributes include 'Subject_Name', 'Subject_Age', 'Subject_Sex'.

3. Forensic Lab

Figure 5. Forensic lab

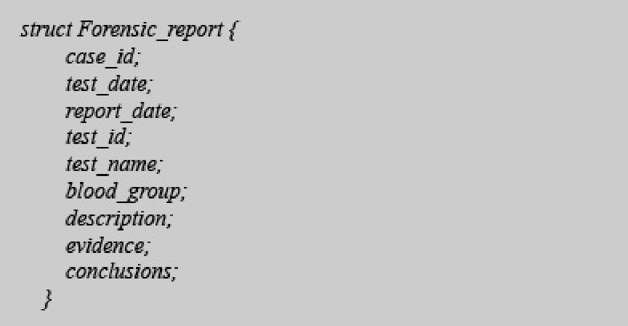


```
struct Forensic_lab {
      Lab_ID;
      Area_code;
      Lab_name;
}
```

'Forensic Lab' is a structure to hold the information about the forensic lab in which the forensic tests are being conducted. It has the attributes 'Lab_ID', 'Area_code', 'Lab_name' **(Figure 5)**. Unlike the previous structure, this structure does not have a unique ID generated by a hash function. The primitive idea behind not utilizing a hash function for the forensic lab is because we did not feel the information related to the lab was a confidential or sensitive information. Whereas information pertaining to an individual or a subject is treated as sensitive information globally.

4. Forensic Report

Figure 6. Forensic report



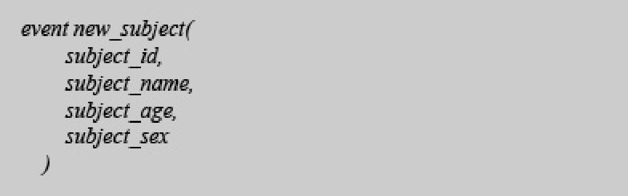
```
struct Forensic_report {
      case_id;
      test_date;
      report_date;
      test_id;
      test_name;
      blood_group;
      description;
      evidence;
      conclusions;
  }
```

'Forensic Report' structure encompasses the details unique to a particular forensic report. A forensic report will have the details pertaining to case **(Figure 6)**.

Till now each entity were a discrete unit, storing different attributes relevant to each of them. Later we will see how these are mapped to each other.

5. Event new_subject

Figure 7. New subject



```
event new_subject(
      subject_id,
      subject_name,
      subject_age,
      subject_sex
  )
```

Events provide a way for contracts to communicate and emit information about specific occurrences or actions that take place within the contract. They allow external entities, such as off-chain applications or user interfaces, to be notified when a specific event occurs on the blockchain **(Figure 7)**.

Whenever a new subject is added, the basic details of the subject, namely, subject ID, subject name, subject age, and subject sex, are sent to other application communicating to the smart contract whenever a new subject is added to the blockchain using the rules of the smart contract.

6. Mappings

a map is a data structure that allows you to associate values with unique keys. It is similar to a dictionary or an associative array in other programming languages. We have to make sure that we map the correct subject to the correct forensic report. Then we have to map the report to the forensic lab where testing has been done.

There are several reasons for using solidity since mapping is involved:

1. Efficient Data Retrieval: Mapping allows for efficient retrieval of values based on their corresponding keys. Solidity uses a hashing mechanism behind the scenes to map keys to their respective values, making look-ups fast and constant time (O(1)).
2. Easy Data Association: Mapping allows you to associate values with unique keys. This is particularly useful for scenarios where you need to establish relationships or mappings between different entities, such as addresses and balances, user IDs and data, or any other key-value pairs.
3. Automatic Key Existence Check: When accessing a value in a mapping, Solidity automatically checks if a value exists for the provided key. If no value is explicitly assigned, the default value for the value type is returned. This eliminates the need for manual existence checks and simplifies your code.
4. Dynamic Size: Mappings in Solidity can grow or shrink dynamically as keys and values are added or removed. This flexibility allows you to handle changing data requirements without explicitly defining the size upfront, unlike arrays or fixed-size data structures.
5. Security and Integrity: Solidity mappings provide inherent security features. The mapping data is stored on the blockchain and is tamper-proof, ensuring the integrity and immutability of the stored data. Additionally, the use of mappings prevents potential errors, such as duplicate keys, that can occur with other data structures.

7. Add Subject

This function takes in the required details of a subject as input parameters. It then generates a unique ID via hashing function (keccak-256 in our case). and before mapping it to forensic report, the address of user is validated whether the subject details are from the authorized personnel only. And if the validation is affirmative then the details of the subject are mapped to the report, else the details are removed from the memory.

Any details which is not mapped to a certain report is removed from the memory.

8. Add Report

This function adds the report to the blockchain.

RESULTS AND DATA DESCRIPTION

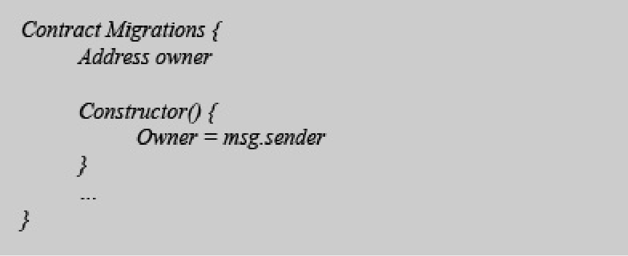
Description of sample data-set: We have used Ganache as our local/private blockchain network which provides us with some sample accounts with unique account address and private key.

9. Request Access

The aforementioned function serves the purpose of verifying the requesting user's address for access to the report. It performs an authorization check, and if the user is deemed authorized, the function proceeds to retrieve and return the report. This mechanism ensures controlled access to the report based on user authorization, enhancing security and confidentiality measures within the system. An event is emitted which provides access to the report.

10. Migration Contract

Figure 8. Migration contract



```
Contract Migrations {
        Address owner

        Constructor() {
                Owner = msg.sender
        }
        ...
}
```

'Migration Contract' encapsulates a set of functions designed to facilitate the transfer of ownership of a forensic report to authorized personnel. The intended structure entails that the individual responsible for inputting the subject details in the report, upon its completion, transfers the ownership exclusively to the investigation department **(Figure 8)**. This mechanism ensures that only authorized entities have access to the information, mitigating the risk of compromise or unauthorized disclosure of the report's contents. By enforcing strict ownership transfer protocols, the contract upholds the confidentiality and integrity of the forensic data, bolstering the overall security framework within the system.

11. Modifier

We use a modifier to restrict the access to the forensic details. For the transfer of ownership, the modifier checks if it is the current owner who is transferring the ownership.

12. Upgrade

This function takes the address of the new owner as input and transfers the ownership. Once the ownership is transferred to the investigation department, the person who conducted the forensic test loses the ownership of the report and he/she cannot make any modifications to it.

Why Solidity

several reasons contribute to Solidity for creating this blockchain-based forensic report system:

1. Immutable and Tamper-Proof: Solidity is specifically designed for smart contract development on blockchain platforms like Ethereum. By leveraging blockchain technology, the forensic report becomes immutable and tamper-proof. Once the report is recorded on the blockchain, it cannot be altered or tampered with, ensuring the integrity and authenticity of the information it contains.
2. Transparency and Auditability: Solidity-based smart contracts provide transparency and auditability features. Every action related to the forensic report, such as ownership transfers or updates, is recorded on the blockchain as a transaction. This allows for easy traceability and audit of the report's history, making it more accountable and verifiable.
3. Enhanced Security: Solidity enables the implementation of robust security measures within the smart contract. By using cryptographic algorithms and public-key cryptography, sensitive data within the forensic report can be securely stored and accessed only by authorized entities. The inherent security features of Solidity and the underlying blockchain technology enhance the overall security of the forensic report.
4. Automation and Efficiency: Solidity allows the automation of certain processes within the forensic report system. For example, ownership transfers can be programmed to occur automatically based on predefined conditions or rules.

This streamlines the workflow and eliminates the need for manual intervention, increasing efficiency and reducing the potential for human error.

5. Interoperability and Integration: Solidity-based smart contracts can interact with other smart contracts and decentralized applications (DApps) on the blockchain. This enables seamless integration with other components or systems within the forensic report ecosystem, promoting interoperability and enabling the development of a comprehensive and interconnected network of applications.

Hence, we ensure the robustness and trustworthiness framework for managing and safeguarding forensic data, and enhancing the overall integrity and reliability of the report.

RESULTS AND DATA DESCRIPTION

Description of sample data-set: We have used Ganache as our local/private blockchain network which provides us with some sample accounts with unique account address and private key.

Data analysis: Smart contracts are self-executing contracts with the terms of the agreement between pathologist and police being directly written into lines of code. Ganache allows developers to deploy smart contracts and test them in a local blockchain environment. Data analysis can be done on the smart contracts to identify vulnerabilities and improve their security.

Discussion and Results: The proposed work involved designing and developing a blockchain-based system using Solidity and Truffle. The system was designed to be secure, transparent, and tamper-proof, ensuring that forensic investigators could rely on the accuracy and authenticity of the data stored on the blockchain.

By using blockchain technology, the work aimed to improve the efficiency and accuracy of forensic investigations. The immutable nature of the blockchain ensures that all data is recorded accurately and cannot be altered or deleted, reducing the risk of errors or tampering. This can help investigators to identify and solve crimes more quickly and effectively.

The blockchain-based system was designed to integrate seamlessly with existing forensic tools and processes, allowing investigators to use the system alongside other tools they may already be using. This can help to streamline investigations and make the process more efficient.

The proposed work demonstrated the potential for blockchain technology to be used in forensic investigations, and its potential to have a wider impact on the field of law enforcement and criminal justice. As more organizations begin to explore the use of blockchain technology, the work could be seen as a blueprint for future developments in this area.

Overall, the proposed work demonstrated the potential for blockchain-based forensics using Solidity and Truffle to improve the efficiency.

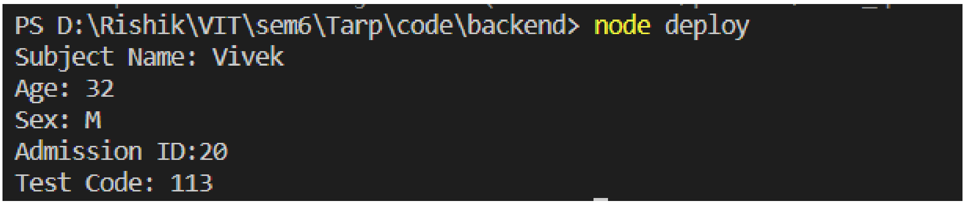
DISCUSSION

We executed the smart contract using a set of sample data. The smart contract was deployed on a local network, specifically on the server address HTTP://127.0.0.1:7545, utilizing the Ganache Network. Notably, the deployment of the contract on Ganache incurred a cost of 0.00479401ETH. This expenditure was necessary to initialize and activate the contract, ensuring its proper functioning within the local blockchain environment. By conducting this deployment on Ganache, we were able to simulate a realistic blockchain scenario without incurring expenses on the actual Ethereum network. There were several reasons we chose Ganache for testing our Smart Contract:

1. Speed and Determinism: Ganache runs locally on your machine, making transactions and contract deployments near-instantaneous. It also ensures determinism, meaning that the blockchain state remains the same every time you start Ganache, enabling predictable testing and debugging.
2. Flexibility and Control: Developers have control over the blockchain's behavior, such as the number of accounts, gas limits, block times, and network conditions. This allows for easy customization and testing of various scenarios.
3. Testing and Debugging: Ganache provides powerful tools for testing and debugging smart contracts. It integrates well with popular development frameworks like Truffle, allowing seamless integration into the development workflow.
4. Realistic Simulation: Despite running locally, Ganache simulates the behavior of the Ethereum network, including mining, transaction processing, and account interactions. This allows developers to test their applications under realistic conditions before deploying them on the main Ethereum network.

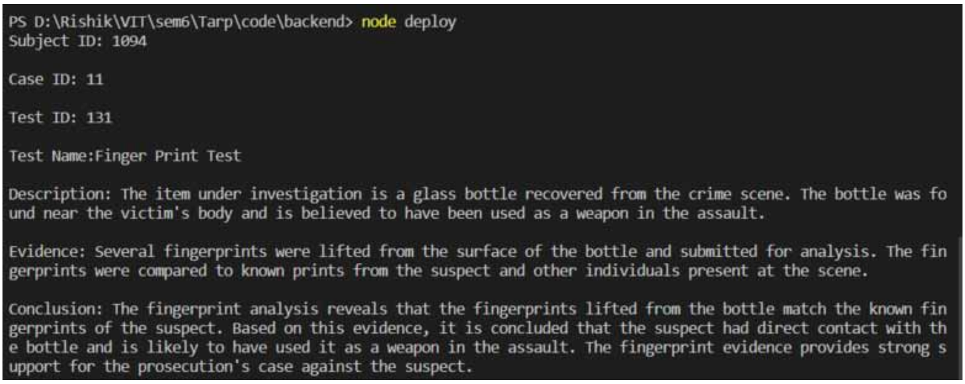
Following are the depiction of how the details were stored in the blockchain:

Figure 9. Viewing subject details



```
PS D:\Rishik\VIT\sem6\Tarp\code\backend> node deploy
Subject Name: Vivek
Age: 32
Sex: M
Admission ID:20
Test Code: 113
```

Figure 10. Viewing report details



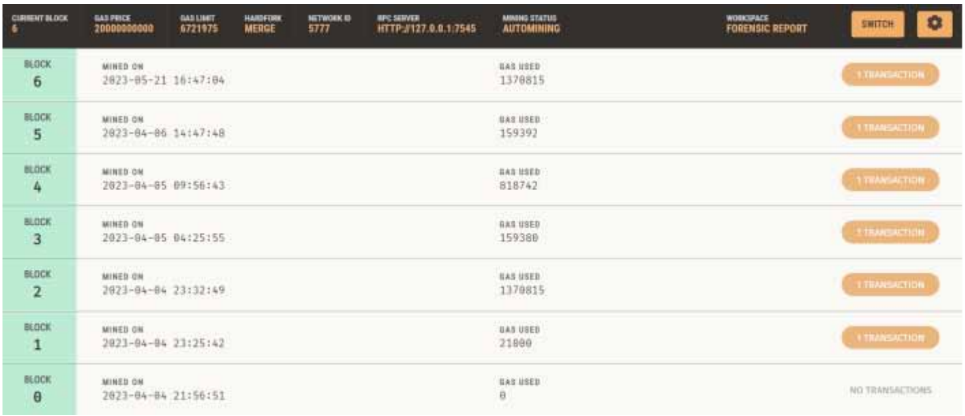
```
PS D:\Rishik\VIT\sem6\Tarp\code\backend> node deploy
Subject ID: 1094

Case ID: 11

Test ID: 131

Test Name:Finger Print Test

Description: The item under investigation is a glass bottle recovered from the crime scene. The bottle was fo
und near the victim's body and is believed to have been used as a weapon in the assault.

Evidence: Several fingerprints were lifted from the surface of the bottle and submitted for analysis. The fin
gerprints were compared to known prints from the suspect and other individuals present at the scene.

Conclusion: The fingerprint analysis reveals that the fingerprints lifted from the bottle match the known fin
gerprints of the suspect. Based on this evidence, it is concluded that the suspect had direct contact with th
e bottle and is likely to have used it as a weapon in the assault. The fingerprint evidence provides strong s
upport for the prosecution's case against the suspect.
```

The data stored over the blockchain network can be retrieved by the authorized personnel as a JSON object **(Figure 9)** and **(Figure 10)**.

Figures 9 and 10 give the visual display of the data that is stored within the blockchain network through the execution of our smart contract in a simple terminal window. Network over which the data is stored can be private network or a public, although private network would be advised. This data can be retrieved or accessed only by the authorized investigative department within that network.

We used web3.js library to get the details of the report in JSON format. These details can only be accessed if and only if a person's account address has been given the ownership. In addition to this, every transaction executed on the network is meticulously recorded and stored within blocks. These blocks serve as immutable records of the transaction history. Ganache provides an easy and straightforward means to visualize the logs associated with each transaction conducted on the network. This functionality enhances the transparency, traceability, and overall visibility of transactions within the Ganache network, contributing to a more robust and accountable blockchain ecosystem.

Figure 11. Transaction logs on the local network



CURRENT BLOCK 6
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MERGE
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE FORENSIC REPORT

BLOCK	MINED ON	GAS USED	
6	2023-05-21 16:47:04	1370815	1 TRANSACTION
5	2023-04-06 14:47:48	159392	1 TRANSACTION
4	2023-04-05 09:56:43	818742	1 TRANSACTION
3	2023-04-05 04:25:55	159380	1 TRANSACTION
2	2023-04-04 23:32:49	1370815	1 TRANSACTION
1	2023-04-04 23:25:42	21000	1 TRANSACTION
0	2023-04-04 21:56:51	0	NO TRANSACTIONS

Figure 11 depicts the log activity of all the transactions done on the network on which the smart contract was deployed. The term 'transaction' here refers to the execution of any function in the smart contract, either by the owner or by non-owner by any illicit means. These logs are stored on the blocks forever and cannot be modified by any currently prevailing computing power.

This transparency allows for the detection of any unauthorized or suspicious activities, as any irregularities or inconsistencies in the transaction history can be easily identified and investigated. Logs enable forensic analysis and incident response in case of security breaches. By examining the transaction logs, security professionals can trace the origin and impact of a security incident, identify compromised accounts or smart contracts, and take appropriate measures to mitigate the damage. Furthermore, transaction logs aid in the identification and prevention of fraudulent activities. By monitoring the logs, patterns of fraudulent behavior can be detected, and preventive measures can be implemented to protect the network and its users. This could include the identification of phishing attempts, suspicious transaction patterns, or unauthorized access attempts. By providing a transparent and audit-able record of transactions, logs enable participants to verify the legitimacy and correctness of transactions, reducing the risk of tampering or fraud. This accountability discourages malicious actors from engaging in unauthorized activities, as their actions can be easily traced and linked back to their identities.

We ran a security check analysis on SolidityScan. SolidityScan is a popular online service that provides static analysis of Solidity smart contracts on the Ethereum blockchain. It analyzes the code for potential vulnerabilities, security risks, and best practices violations. While SolidityScan can be a useful tool for identifying common coding errors and security issues. Our smart contract got a score of 4 out 5 for potential weak vulnerabilities and 0 medium and 0 high vulnerability risks.

Forensic investigation is a sensitive field where reliability of data is crucial. There is need to develop a tamper proof system which can be relied upon with minimal human interference. Adding blockchain technology to digital forensics inculcates confidence and credibility to the forensic data. All the changes are stored as transaction history in a distributed network of blocks which are traceable and unalterable. The transaction history is verifiable and hence adds authenticity to the forensic data.

Overall, the paper emphasizes on handling the existing problem of mishandling and unethical modifications to the forensic data. By transferring the ownership, the system ensures that forensic data is with the investigating department or any other authority who is not concerned with the modifying of data, but making inferences from the data they have received. In order to make any changes to the forensic data, the organization must demand transfer of ownership back from the current owner. All the transfer of ownership and changes made to the data remain saved in the distributed network and are traceable if any felony or discrepancy is found or need to be checked for.

LIMITATIONS

Scalability: This paper does not encompass a discussion on the potential for scaling the implementation or the methodologies required for scaling the system. Furthermore, it does not delve into the challenges that may arise during the large-scale implementation of the system.

Standard Protocols: The paper does not address the standard protocols that an organization must adhere to during the implementation of this system.

Government Regulations: Forensic investigation is intricately entwined with the legal framework of a specific country. Each nation possesses its own set of regulations and policies governing data privacy. The paper does not indulge in any political aspects of the matter and strictly adheres to, as the title conveys, protecting the forensic data from any modifications that has not been made by an authorized body.

Developing a private network: The paper exclusively concentrates on the development of smart contracts and functionalities aimed at securing forensic data. Developing a private blockchain network or deploying of a smart contract falls beyond the scope of this paper.

CONCLUSION

Blockchain is the ideal option for keeping and securing the forensic information since it offers the finest security, integrity, transparency, and audit. Due to the distributed nature of the blockchain, which makes it difficult to change any individual block, it reduces dispute and fosters greater belief[8]. The most practical approach for forensics in the digital age is blockchain. According to our analysis, blockchain technology is still being applied in innovative ways in the field of digital forensics. Only 11 research publications addressing digital forensics in cryptocurrencies are included in this assessment. Only four of the five digital forensic phases are covered by the research from the 11 chosen publications. In the presentation phase, no research papers have yet been discovered. Another issue that is worth mentioning is that none of the research papers on the collection and preservation phase address the issue of preserving the blockchain's related evidence. Aside from our main findings, we also outline several issues that can be considered as open challenges for digital forensic investigation in cryptocurrency technology.

FUTURE WORK

Optimization

We need to decide whether to save all blockchain evidence or perform optimization and preserve the best evidence while tackling the preservation issue.

- The bitcoin environment should be given its own official forensic framework.
- The cryptocurrency environment uses a wide range of platforms and technologies.
- For processing massive data on the blockchain for cryptocurrencies, clustering algorithms are required.
- For further investigation of bitcoin forensics, the creation of a test bed is required.
- Assistive technologies for health care can also use the proposed system and provide more secure, transparent services to the user and the other end users.

Meeting the Growing Demand

The growing demand and expansion of blockchain technology poses certain challenges with respect to the power consumption corresponding to various consensus algorithms used. The most common types of consensus algorithms are: *proof-of-*

work (PoW), proof-of-stake (PoS), and *proof-of-authority (PoA).* Proof-of-work is the most commonly known and utilized consensus algorithm, but it is also the most power consuming mechanism. Bamakan et al. Discusses various studies that have been done on estimating the power requirements for implementing proof of work algorithm on a large scale. It is safe to say that proof of work is not a suitable consensus algorithm when there is a growing demand for blockchain network and a lot of organizations are consuming power for every transaction performed on the network. In addition to computing power, proof of work is also a time-consuming process, which is one of the reasons for its high security, but for a large scale implementation we need an algorithm that

Proof of Stake resolves the issue posed by proof of work by eliminating the need for each node to perform mining. This removes the need for high computing power and high time consumption.

An increase in demand also comes with a high risk for cyber threats. The most popular types of cyber-attacks are *51% attack* and *Sybil attack* [13]. PoW and PoS are prone to the former threat, that is 51% attack. Proof of Authority overcomes this vulnerability by establishing a sense a of authority among the nodes where a few chosen nodes are given higher authority and preference whom we trust are inaccessible to anyone. Although 51% attack is minimized by PoA, it still is prone to Sybil attack.

Hasanova et al. discusses about minimizing the sybil attack by giving unequal power to different nodes. This idea seems feasible on a small scale but has its own challenges when there are more users and nodes. One major challenge to implement the idea of unequal power is to decide how much power to be given to each node when the network is vast or there are large number of nodes. Although this can be achieved by utilizing various artificial intelligence techniques and machine learning algorithms. This is further discussed in the next section.

Integrating Blockchain With AI

The term decentralized AI [11] is used for describing a combination of AI and blockchain technology where AI decisions are made on secured data that is transacted and stored on a blockchain network. Artificial intelligence can play 2 important roles in blockchain technology:

1. Artificial intelligence techniques and algorithms can be used with many consensus algorithms to improve the latter's efficiency. More discussion on the topic is done ahead in this section.
2. Artificial intelligence can be used with blockchain to analyze and process large amounts of data to perform many tasks such as implementing a decentralized

robotic system [9]. A decentralized communication system is more efficient than a central communication system within the field of healthcare, as it provides more dynamic performance to the system by allowing multiple AI agents to access different parts of the data at the same time. The discussion and implementation of such processes is outside the scope of the chapter, although further discussion done on how AI can process and utilize large data that is stored on decentralized platform and how the proposed methodology of transferring of ownership improves the performance and reliability of such AI models.

In addition to PoW, PoS and PoA, many other consensus algorithms have been suggested which improved upon existing mechanism but carried their own disadvantages and challenges. AI possess the potential to overcome these challenges in many ways. One of the solutions proposed for protecting PoA from sybil attacks was to give unequal power to different nodes, but this posed a challenge as calculating the optimum power to allocate to each node in a large network can be difficult. AI models can help in allocating right amount of power to each node in an efficient manner.

An improvement to PoA is *Proof-of-Importance (Poi)*[11]. In PoI certain nodes are given higher priority for validating transactions. PoI sets a certain threshold for nodes which must be met in order to consider that node's validation as success. AI is expected to help in determining a suitable value for these thresholds based on the past validations by the nodes.

Proof-of-Estimated-Time (PoET)[11] is another consensus algorithm which sets a random time for each node and the node with the minimum expiration duration is selected a s the leader. The leader node is expected to validate the transactions until its expiration. Once expired PoET again follows the same protocol of allotting random time limits and selecting a new leader. This process keeps on going continuously. This method reduces the time and power consumption significantly as opposed to the existing proof of work algorithm and hence is a suitable algorithm for large scale implementation of blockchain technology. AI has vast potential in improving the efficiency of such algorithms which have greater potential to be used in practical applications. Since time allotment in PoET is randomized, there are chances of the same node to become the leader multiple times. AI can detect fraudulent nodes if certain nodes are becoming leaders more frequently than others and can distinguish more accurately and precisely whether a certain node becoming a leader multiple times is coincidental or if the time allotment protocol has been compromised. This can be achieved by looking for patterns in allotment of time limits or if a particular node is becoming the leader after certain intervals. If there exists a corrupt node which might fraudulently become the leader by compromising the time allotment protocol, then it can validate the fake transactions and hence reliability of the system is reduced. Some machine learning algorithms such as anomaly detection can also aid in reducing such risks.

In the Field of AI-Based Digital Health Communication System

It is important to understand the current flaws in existing digital health systems in order to understand the criticality of blockchain technology in AI-based digital health communication systems. The primary objective of AI is to automate the processes involved in an operation and to take most optimal decisions. For better decisions AI heavily relies on the data that is collected and stored. In current times, the collection and storage of this data is contained by a central authority. By transacting and storing this data on decentralized platform, we ensure better reliabily and authenticity of data. There have been cases where hospitals tamper with patient's data to make higher profits. By implementing Electronic Health Records (EHRs) on a decentralized platform and keeping a tamper-proof record of all transactions as record logs, we avoid such scenario.

The proposed methodology closely correlates to the field of digital healthcare and health communication. There are instances where patients do not prefer or do not consent to their personal data being recorded or shared [12], and hospitals not wanting to share their data records. Many times hospitals are restricted by the consent of the patient to share the data for research, hence there is a decline in the quality of collected data that is used for improving the AI models. Blockchain provides a platform where the data can be stored and be tamper-proof. The proposed methodology further adds to the security and reliability of the data by ensuring that the patients, hospitals and other stakeholders involved are assured that their data is stored outside the control and access of any central authority and any compromising of data can be traced down. In this manner quality of data is assured which results in better performance of AI models.

This in turn helps the AI models to perform better in checking for any fraudulent transactions, tracking any unethical usage of patient records and automating the transfer of ownership and other operations. Other operations can range from responding to patients or providing them updates on their reports, to automating the process of prioritizing the patient queue based on their past records and criticality and severity of their case. Prioritizing which patient needs to be attended to is a very crucial and imperative process and we need that the AI model takes the most reasonable and appropriate decision which is heavily dependent on the quality of data it is trained on. Digital health communication systems often work on large amounts of data which needs to be handled in an efficient manner. Not all data is required for a specific task. Hence it becomes very time consuming to filter and to process which data is needed for a particular task or to train an AI model. AI possesses the capability to itself detect which data it needs for performing tasks and making decisions and can decide whom to give access to the specific parts of data by following the ownership transfer protocol.

Validation of medical reports is another critical operation that can performed by AI, where validation is done by the nodes on the network by using suitable consensus algorithms such as PoI as discussed before. Validating medical reports is an example where we want to be certain only certain authorities get access(ownership) to the report and the people or systems involved in generating the report do not have any further editing access to the report.

Other Fields

The functionality can be extended to other domains such as other government departments where finances and transactions are involved, as well as education sectors where fraudulent money charges may be levied by some institutes. The concept of transferring ownership effectively eliminates access from any entity that may attempt unethical data modification. Consequently, the proposed methodology holds the potential for implementation across any field susceptible to data tampering by unethical actors. The subsequent sections will exclusively center on the application of this methodology for the enhancement of forensic data security.

REFERENCES

Ahmed, M., Reno, S., Akter, N., & Haque, F. (2020). *Securing Medical Forensic System Using Hyperledger Based Private Blockchain.* IEEE. doi:10.1109/ICCIT51783.2020.9392686

Bamakan, S. M. H., Motavali, A., & Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, *154*, 113385. doi:10.1016/j.eswa.2020.113385

BorseY.PatoleD.KukrejaG.ParekhH.JainR. (2021). Advantages of Blockchain in digital forensic evidence Management. Social Science Research Network. doi:10.2139/ssrn.3866889

Chamola, V., Goyal, A., Sharma, P., Hassija, V., Binh, H. T. T., & Saxena, V. (2022). Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management. *Neural Computing & Applications*. doi:10.100700521-022-07087-7 PMID:35310553

Chen, C., Deng, Y., Weng, W., Sun, H., & Zhou, M. (2020). A Blockchain-Based Secure Inter-Hospital EMR Sharing System. *Applied Sciences (Basel, Switzerland)*, *10*(14), 4958. doi:10.3390/app10144958

De Oliveira, M., Reis, L. H. A., Carrano, R. C., Seixas, F. a. V., Saade, D. C. M., Albuquerque, C., De Azevedo Fernandes, N. C. C., Olabarriaga, S. D., Medeiros, D. S. V., & Mattos, D. M. F. (2019). *Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications*. IEEE. doi:10.1109/ICC.2019.8761307

Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems*, *120*, 13–25. doi:10.1016/j.future.2021.02.016

Li, M., Lal, C., Conti, M., & Hu, D. (2021). LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, *115*, 406–420. doi:10.1016/j.future.2020.09.038

Li, S., Qin, T., & Min, G. (2019). Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. *IEEE Transactions on Computational Social Systems*, *6*(6), 1433–1441. doi:10.1109/TCSS.2019.2927431

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, *28*, 44–55. doi:10.1016/j.diin.2019.01.002

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 10127–10149. doi:10.1109/ACCESS.2018.2890507

Su, Q., Zhang, R., Xue, R., & Li, P. (2020). Revocable Attribute-Based Signature for Blockchain-Based Healthcare System. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 127884–127896. doi:10.1109/ACCESS.2020.3007691

Wenhua, Z., Qamar, F., Abdali, T. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: Security issues, healthcare applications, challenges and future trends. *Electronics (Basel)*, *12*(3), 546. doi:10.3390/electronics12030546

Xi, P., Zhang, X., Wang, L., Liu, W., & Peng, S. (2022). A Review of Blockchain-Based Secure Sharing of Healthcare Data. *Applied Sciences (Basel, Switzerland)*, *12*(15), 7912. doi:10.3390/app12157912

Zakzouk, A., El-Sayed, A., & Hemdan, E. E. (2023). A blockchain-based electronic medical records management framework in smart healthcare infrastructure. *Multimedia Tools and Applications*, *82*(23), 35419–35437. doi:10.100711042-023-15152-z