EVIDENCE VAULT: BLOCKCHAIN AND IPFS ENHANCED SECURITY SYSTEM

Syed Amir Hussain[1], Altaf Ur Rahman[2], Syed Abdul Bari[3], Mrs. L. Vaishnavi[4]
[1,2,3]B. E Student, Department of CSE, ISL College of Engineering, India.
[4]Assistant Professor, Department of CSE, ISL College of Engineering, Hyderabad, India.

ABSTRACT: Crime is an illegal activity that is punished by the government, evidence is required to prove the crime. The evidence gained from a crime place is crucial because it serves as proof of the offense. The digitization of evidence is an urgent necessity. In the digital era, the management and integrity of crime evidence present substantial challenges due to risks of tampering and loss of data integrity. Throughout the investigation process, heterogeneous data formats are generated, and the integrity of sensitive data must be maintained as it passes through the various levels of intermediaries that form the Chain of Evidence (CoE). The evidence needs to be tamper-proof and protected against any alterations. To build robust systems with immutability, integrity, and legitimacy, blockchain technology is superior. Using blockchain technology, digital evidence can be transferred between parties without a central authority in a transparent manner. We focused on how blockchain based solutions can help in building a strong secure system. The system is implemented using Ethereum platform to achieve integrity, immutability transparency as well as tampering can be identified by any one at any time. This project explores the integration of blockchain to ensure the authenticity, traceability, and non-repudiation of digital evidence, while employing IPFS to enhance data availability and fault tolerance.

INTRODUCTION

The current project focuses on the essential need of digitizing criminal evidence in the modern digital age, highlighting the importance of preserving the integrity of evidence throughout investigations. The credibility of evidence is seriously compromised by tampering and unlawful access, which has led to the investigation of creative remedies.Conventional approaches to managing evidence have inherent weaknesses that make them prone to manipulation and compromise. The absence of a strong tracking system in the chain of custody procedure gives rise to questions about the veracity of the information provided in court. Furthermore, the laborious and time-consuming document review procedures in conventional methodologies impede the effectiveness of investigations. These limitations need a fundamental change in thinking towards more secure and technologically sophisticated methods. The initiative suggests using blockchain technology to rectify the limitations of conventional approaches. Blockchain is a cryptographic technology that functions as a decentralized and immutable ledger, ensuring safe and transparent recording of transactions. Blockchain does not store all the data in one location, but rather organizes it into blocks of data, each with an own hash code. The blocks are dispersed across numerous computers (nodes), which significantly increases the difficulty of tampering with the data or compromising the whole system. Blockchain has several benefits. Firstly, it is characterized by decentralization, which implies that the data is not held in a single susceptible place. Furthermore, it improves security by storing the data in an encrypted manner that is very resistant to tampering or unauthorized access. Furthermore, it fosters openness by ensuring that all transactions are meticulously documented and accessible to authorized individuals. Furthermore, it guarantees data immutability, signifying that once an entry is documented in the blockchain, it cannot be readily altered. Ultimately, it exhibits resilience to failures since it is capable of maintaining data even in the event of some nodes being inoperative. The project primarily employs the Ethereum blockchain for its resilient smart contract capability. Smart contracts are contractual agreements that are capable of automatically executing predetermined rules and circumstances. Smart contracts in this context improve the security and transparency of the chain of evidence procedure by enforcing rules pertaining to evidence management. The decentralized structure of Ethereum enhances the overall security and dependability of the suggested system, guaranteeing a credible and tamper-proof setting for criminal evidence.

LITERATURE REVIEW

Crime Evidence Over Blockchain Blockchain is a decentralized digital ledger that stores transaction records across a network of computer systems. It employs a secure method of keeping information, making it very resistant to tampering or unauthorized access. The process of collecting, identifying, assessing, analyzing, conserving, and presenting evidence poses significant challenges in the field of forensics. The decentralized structure of the blockchain allows for forensic evidence to be kept in a private network utilizing the blockchain's nodes in a peer-to-peer network. Furthermore, digital forensics will exhibit enhanced security measures, ensuring a higher level of confidentiality. Additionally, the investigative process will become more apparent to those located across the jurisdictional boundary. During the criminal investigation process, dynamic information is saved on the hot blockchain, while static material like videos are preserved in the cold blockchain. We are using Ethereum principles and executing smart contracts in our project.

A Blockchain Based Forensic System for IoT Sensors using MQTT Protocol Due to the emergence of the Internet of Things (IoT), several IoT end devices have been introduced to the market. However, these devices often suffer from limited computation and storage capabilities. As a result, the lightweight MQTT protocol is often used. Nevertheless, the lightweight nature of IoT sensors using the MQTT protocol renders them susceptible to several malicious attackers, due to their inherent lack of security. Digital forensics is a field that use scientific inquiry to gather evidence of digital crimes and assaults. It may also be used to analyze the methods used by criminals in order to develop more robust defenses against attacks on Internet of Things (IoT) devices. Nevertheless, existing IoT forensic solutions often lack precision and system reliability. This paper proposes a forensic system for IoT sensors that utilizes blockchain technology and the MQTT protocol. The system ensures a comprehensive process from collecting evidence to protecting it, analyzing and categorizing it, and maintaining evidence integrity through federated blockchains. Additionally, the system employs machine learning to assess the severity of harm to the sensor, generating feedback that can be utilized to develop countermeasures against threats and optimize the allocation of monitoring resources.

Blockchain driven Evidence Management System When a recognizable offense like as murder, kidnapping, rape, theft, etc. occurs, the victim or a representative must electronically file a first information report (e-FIR) with the police station. Because the e-FIR database is centralized, there is a risk of the offense's record being hacked and bogus e-FIRs being intentionally recorded. The e-FIR database has significant challenges regarding data openness and integrity. The Indian government initiated the nationwide implementation of the Crime and

Criminal Tracking Network and Systems (CCTNS) in 2009, which serves as a highly effective e-governance system. This article presents a blockchain-based approach for managing both cognizable and non-cognizable complaints. The discussion will focus on the technological and security aspects of blockchain, using real-world examples from past occurrences. The police will submit an electronic First Information Report (e-FIR), which will undergo verification by the authorities. Once the FIR is approved, it will be encoded and securely saved as a hash, along with the timestamp and hash of the subsequent block. The security of blockchain lies in its mechanism that prevents any modifications to the FIR without the presentation of proof of work and the approval of a consensus vote, requiring a majority agreement among the blockchain participants. The hash will be saved in Ethereum smart contracts. The results of our study reveal a compromise between the quantity of transactions included in a single block on the blockchain ledger and the amount of security provided by different hashing algorithms for the offense data.

Two-Level Blockchain System for Digital Crime Evidence Management Digital evidence, including information obtained from closed-circuit television (CCTV) and event data recorders, has significant value in criminal investigations and serves as conclusive evidence during trials. Nevertheless, there are potential hazards associated with storing digital evidence collected during a case investigation on a physical hard disk drive until it is presented in court. Prior research has mostly concentrated on the unified administration of digital evidence inside a centralized system. However, in the event of a cyber assault on the central server, critical operations and investigative data might potentially be compromised. Hence, it is essential to effectively handle digital evidence and investigative data by using blockchain technology inside a decentralized system setting. However, the storage of substantial material, such as evidentiary recordings, in a blockchain leads to an increase in the quantity of data that has to be processed inside a single block before it can be formed. This, in turn, results in a decline in speed. Hence, we suggest implementing a two-tier blockchain architecture that segregates digital evidence into hot and cold blockchains. During the criminal investigation process, dynamic information is saved on the hot blockchain, while static material like videos are preserved in the cold blockchain. In order to assess the system, we conducted measurements on the storage and inquiry processing performance of digital criminal evidence movies, taking into account the varying capabilities inside the two-level blockchain system.

xCRM: Blockchain Interoperable Crime Report Management System By Utilizing Hyperledger Cacti & Private Data Collection (PDC) Bringing criminals to court may be a complex endeavor, particularly when confidential reporter information and sensitive case data are exposed. This procedure may need collaboration with foreign law enforcement agencies, especially if the offender escapes to another country. In order to address this problem, it is essential to implement an interoperable crime management system. This research suggests the implementation of a crime management system that utilizes blockchain technology to enable safe and decentralized communication across several blockchain-based platforms. This system guarantees anonymity, transparency, and immutability. We propose a systematic approach for reporting crimes, managing evidence, conducting forensic testing, facilitating collaboration among investigation agencies, and sharing resources. Our methodology allows individuals to report incidents in two modes: anonymous mode, which enables the submission of information to the police without revealing the identity of the informant, or generate mode, which initiates the creation of a First Information Report (FIR) and subsequent procedures. In order to safeguard the confidentiality of our data, we have used Hyperledger Fabric Private Data Collection (PDC) for every report and inquiry. The PDC will include the team leader, investigation officer, reporter, and any other pertinent users as members. Interactions will only take place in the designated channel assigned to each report, and any files or supplementary material will be transmitted via the PDC. This system utilizes Hyperledger Cacti to provide interoperability and facilitate inquiry and cooperation with many entities, such as courts, forensics, and special investigative agencies, including those from foreign jurisdictions. This suggested approach is very effective and efficient, significantly improving the performance of blockchain networks.

SYSTEM ARCHITECTURE:

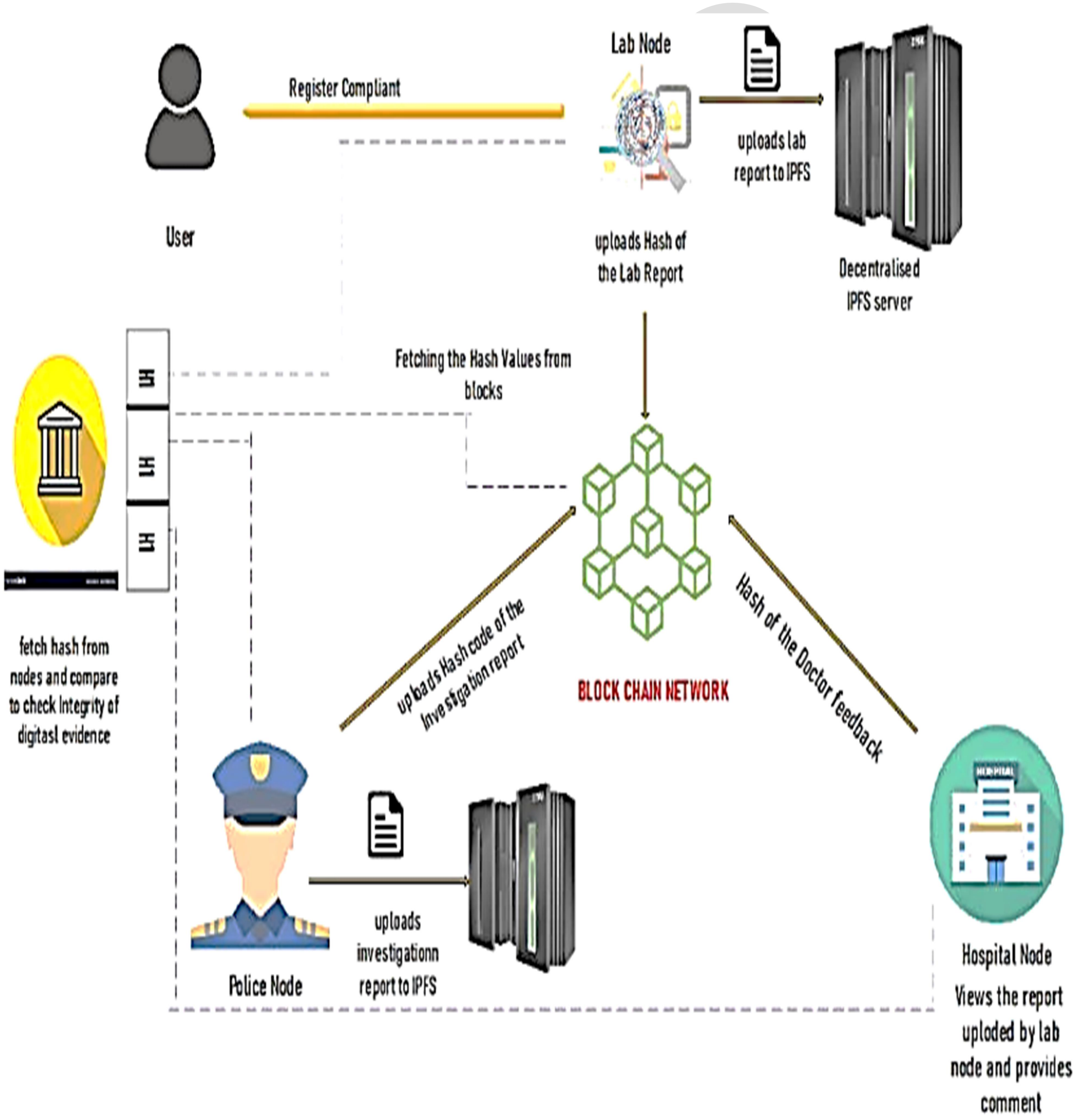

User
Register Compliant
Lab Node
uploads lab report to IPFS
uploads Hash of the Lab Report
Decentralised IPFS server
Fetching the Hash Values from blocks
fetch hash from nodes and compare to check Integrity of digitasl evidence
uploads Hash code of the Investigation report
BLOCK CHAIN NETWORK
Hash of the Doctor feedback
Police Node
uploads investigationn report to IPFS
Hospital Node
Views the report uploded by lab node and provides comment

Fig. 1: System Architecture.

DATA FLOW DIAGRAM (DFD):

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

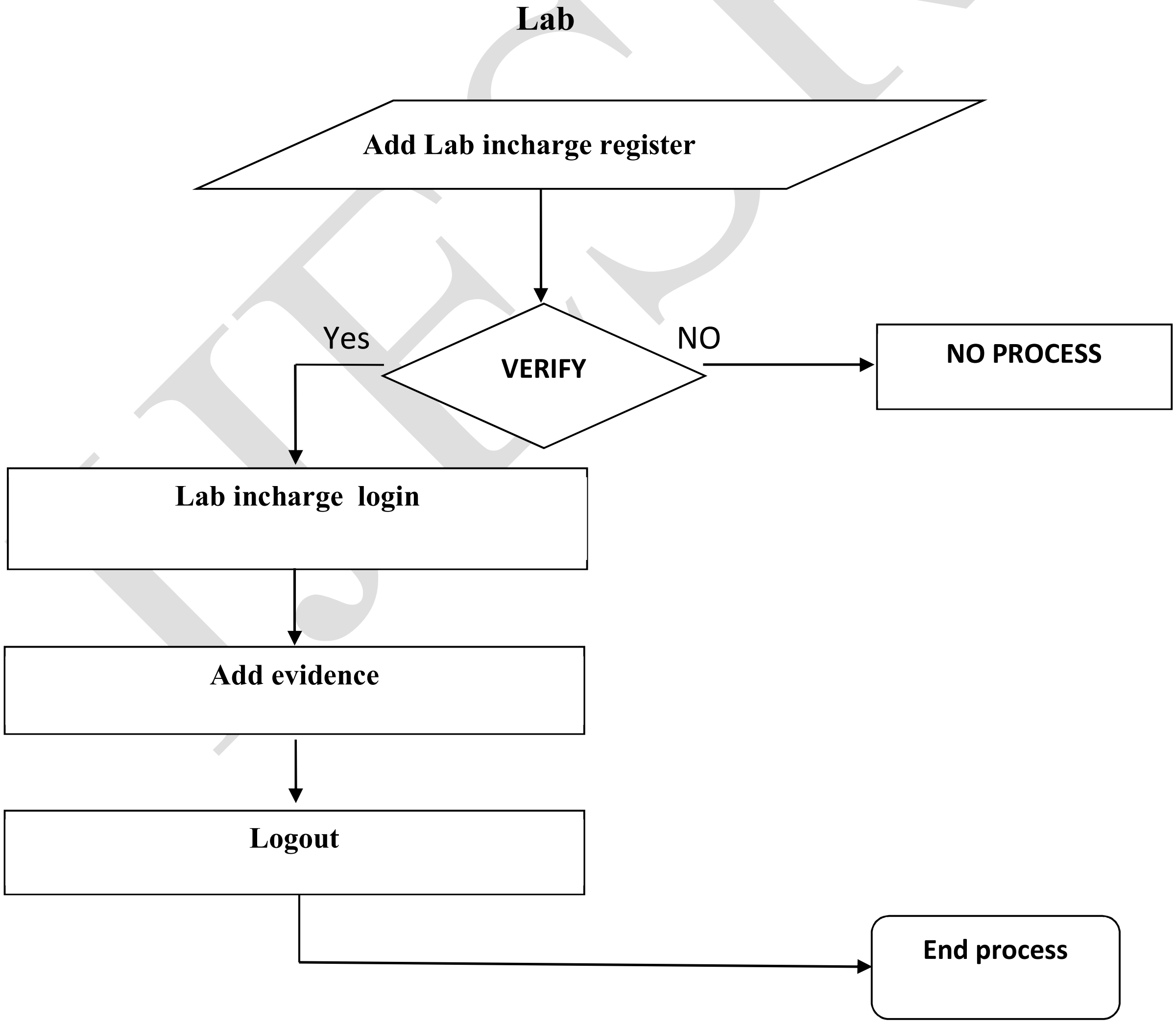


Fig. 2 Dataflow Diagram of Lab.

Hospital

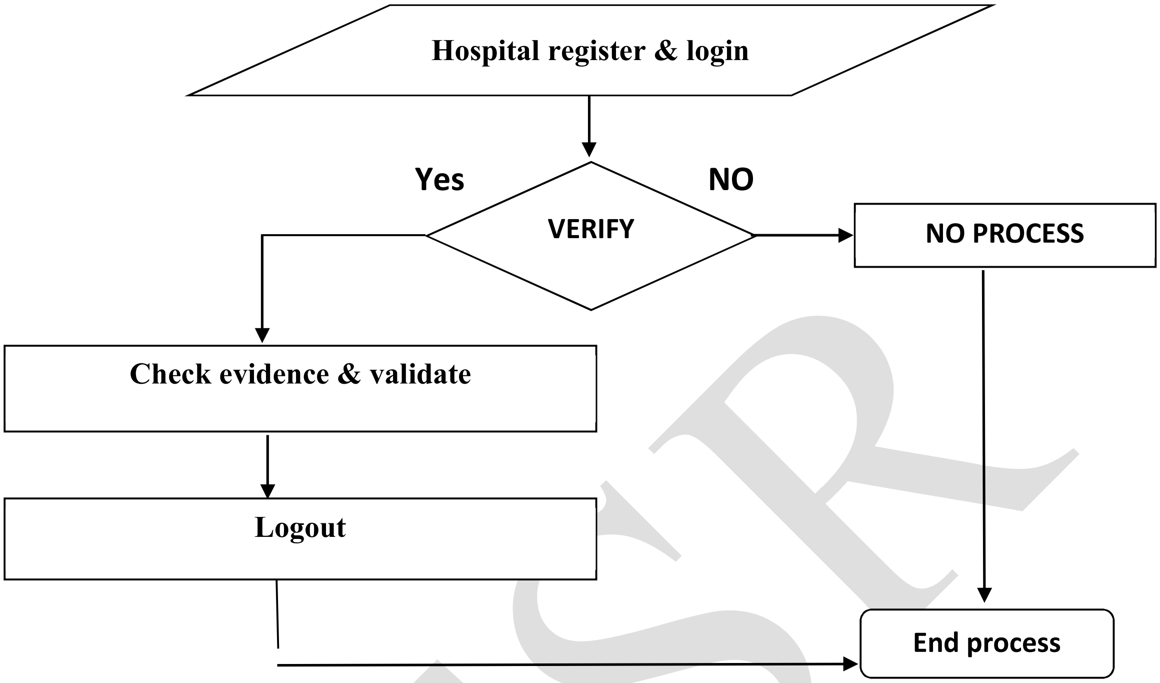


Fig 3 Dataflow Diagram of Court.

Police

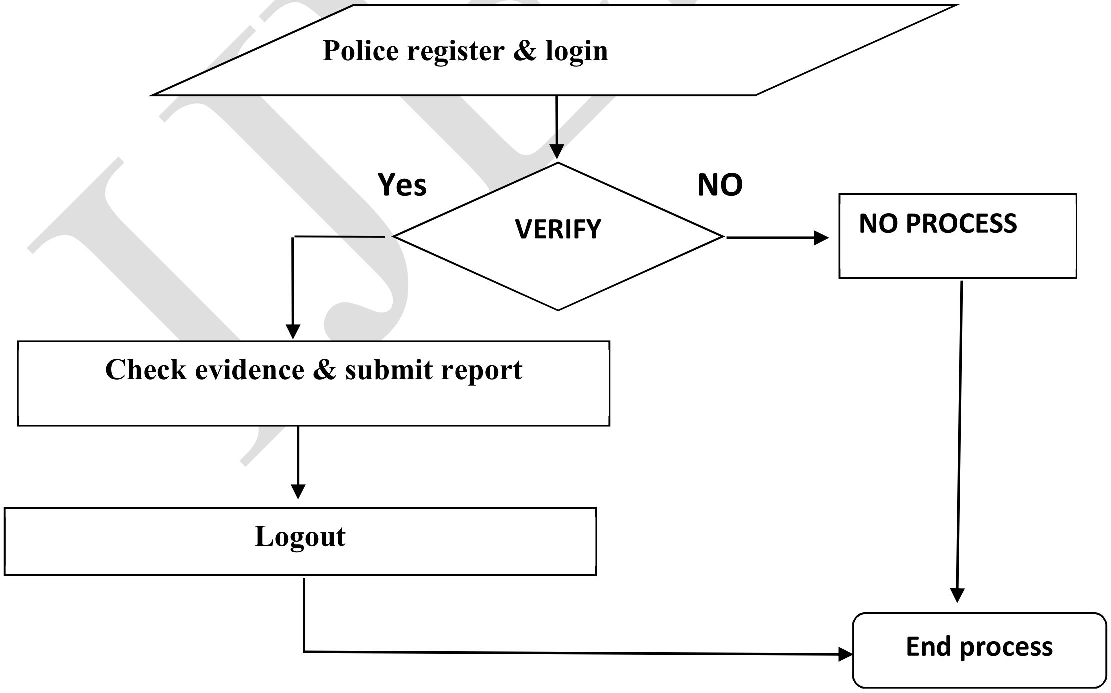


Fig 4 Dataflow Diagram of Police.

Court

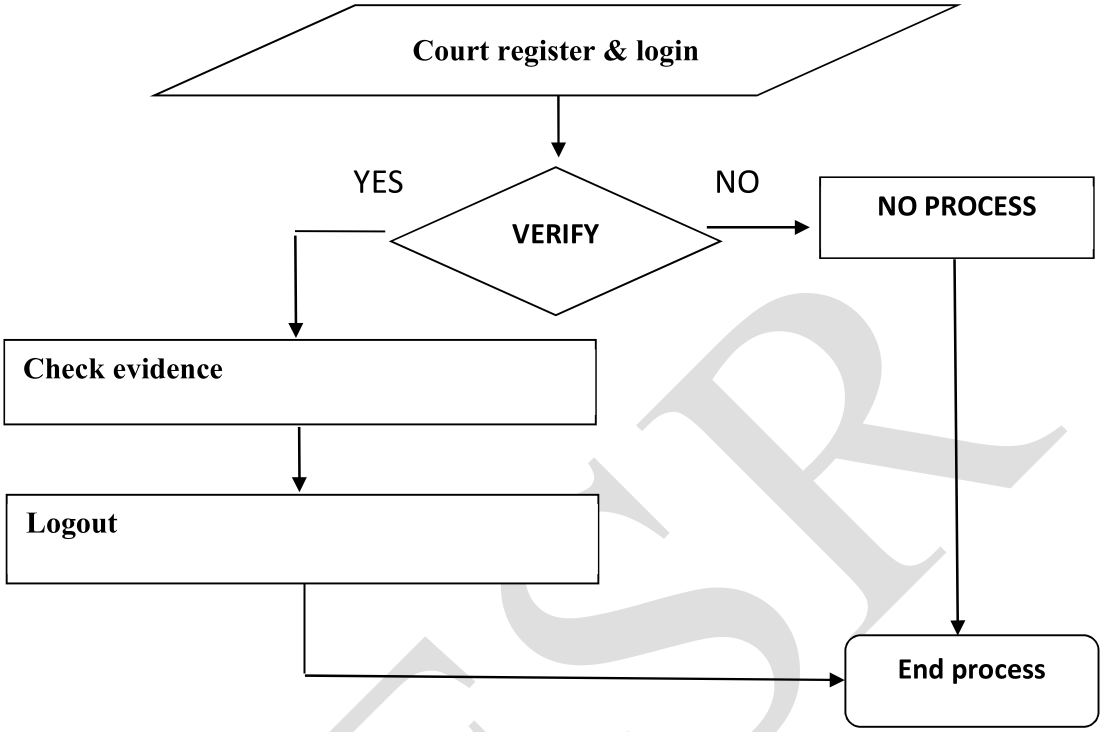


Fig 5 Dataflow Diagram of Court.

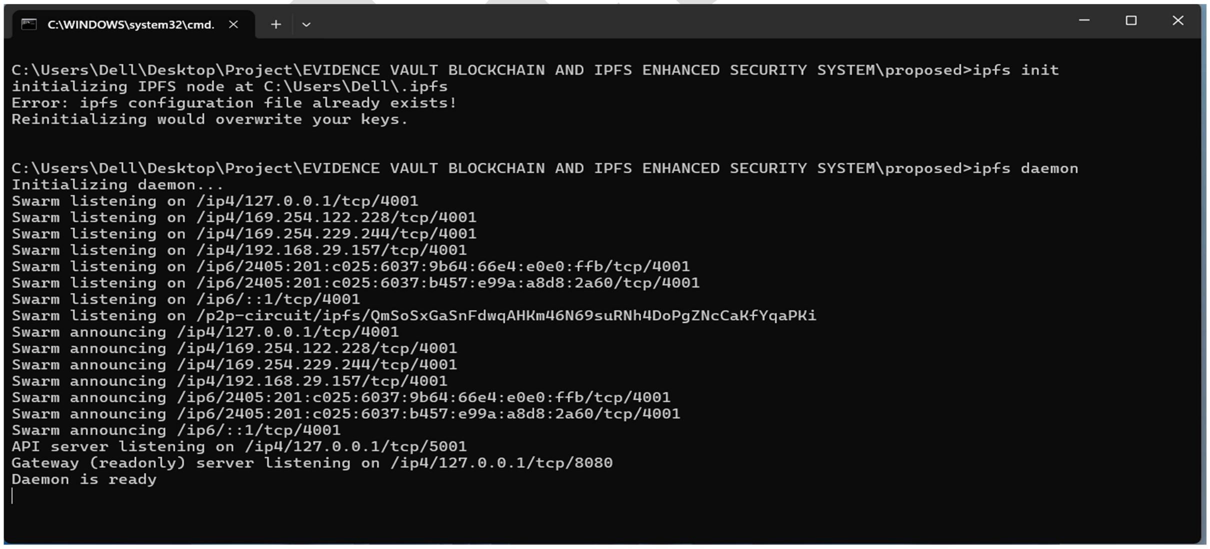
SYSTEM TESTING

System testing, also known as system-level tests or system-integration testing, is the assessment that is carried out by a quality assurance (QA) team in order to evaluate the interaction that occurs between the various components of an application within the context of the whole, integrated system or application. The process of ensuring that a program is able to carry out its functions in a manner that is consistent with its original design is known as system testing. A specialized examination of the operation of an application is carried out at this step, which is a kind of testing known as black box testing. It is the responsibility of system testing to guarantee that all forms of user input produce the anticipated outcome across the whole of the program.

TEST CASES:

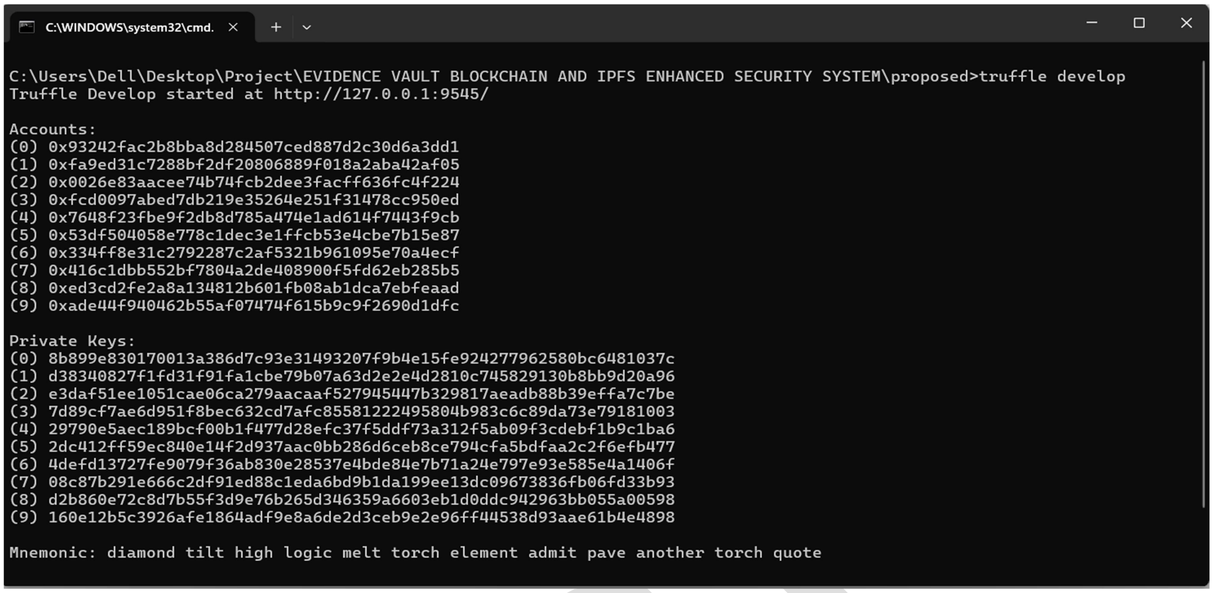
S.NO	INPUT	If available	If not available
1	Add evidence	Lab incharge can add evidence and sent reports to hospital	There is no process
2	Check evidence & validate	Hospital can check evidence & validate and sent reports to police	There is no process
3	Check evidence & submit report	Police can check evidence & submit report to court	There is no process
4	Check evidence	Court can check evidence	There is no process

OUTPUT SCREENS



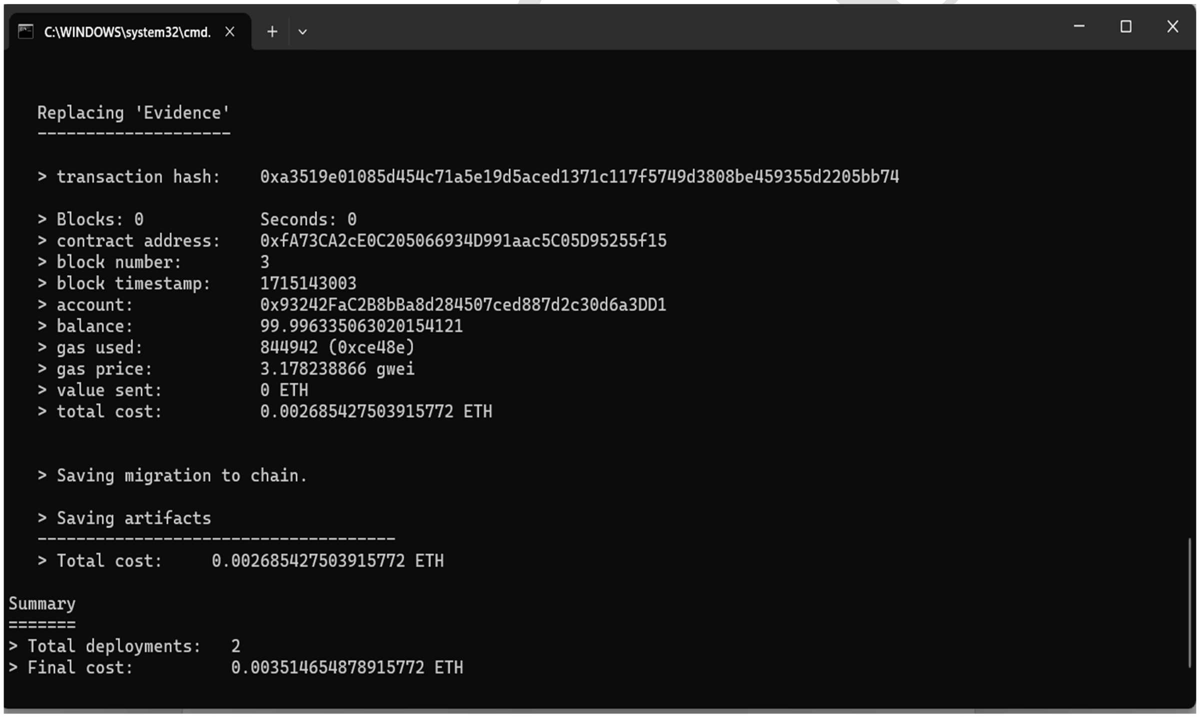
```
C:\Users\Dell\Desktop\Project\EVIDENCE VAULT BLOCKCHAIN AND IPFS ENHANCED SECURITY SYSTEM\proposed>ipfs init
initializing IPFS node at C:\Users\Dell\.ipfs
Error: ipfs configuration file already exists!
Reinitializing would overwrite your keys.


C:\Users\Dell\Desktop\Project\EVIDENCE VAULT BLOCKCHAIN AND IPFS ENHANCED SECURITY SYSTEM\proposed>ipfs daemon
Initializing daemon...
Swarm listening on /ip4/127.0.0.1/tcp/4001
Swarm listening on /ip4/169.254.122.228/tcp/4001
Swarm listening on /ip4/169.254.229.244/tcp/4001
Swarm listening on /ip4/192.168.29.157/tcp/4001
Swarm listening on /ip6/2405:201:c025:6037:9b64:66e4:e0e0:ffb/tcp/4001
Swarm listening on /ip6/2405:201:c025:6037:b457:e99a:a8d8:2a60/tcp/4001
Swarm listening on /ip6/::1/tcp/4001
Swarm listening on /p2p-circuit/ipfs/QmSoSxGaSnFdwqAHKm46N69suRNh4DoPgZNcCaKfYqaPKi
Swarm announcing /ip4/127.0.0.1/tcp/4001
Swarm announcing /ip4/169.254.122.228/tcp/4001
Swarm announcing /ip4/169.254.229.244/tcp/4001
Swarm announcing /ip4/192.168.29.157/tcp/4001
Swarm announcing /ip6/2405:201:c025:6037:9b64:66e4:e0e0:ffb/tcp/4001
Swarm announcing /ip6/2405:201:c025:6037:b457:e99a:a8d8:2a60/tcp/4001
Swarm announcing /ip6/::1/tcp/4001
API server listening on /ip4/127.0.0.1/tcp/5001
Gateway (readonly) server listening on /ip4/127.0.0.1/tcp/8080
Daemon is ready
```

Fig. 6. Command prompt installing IPFS server.



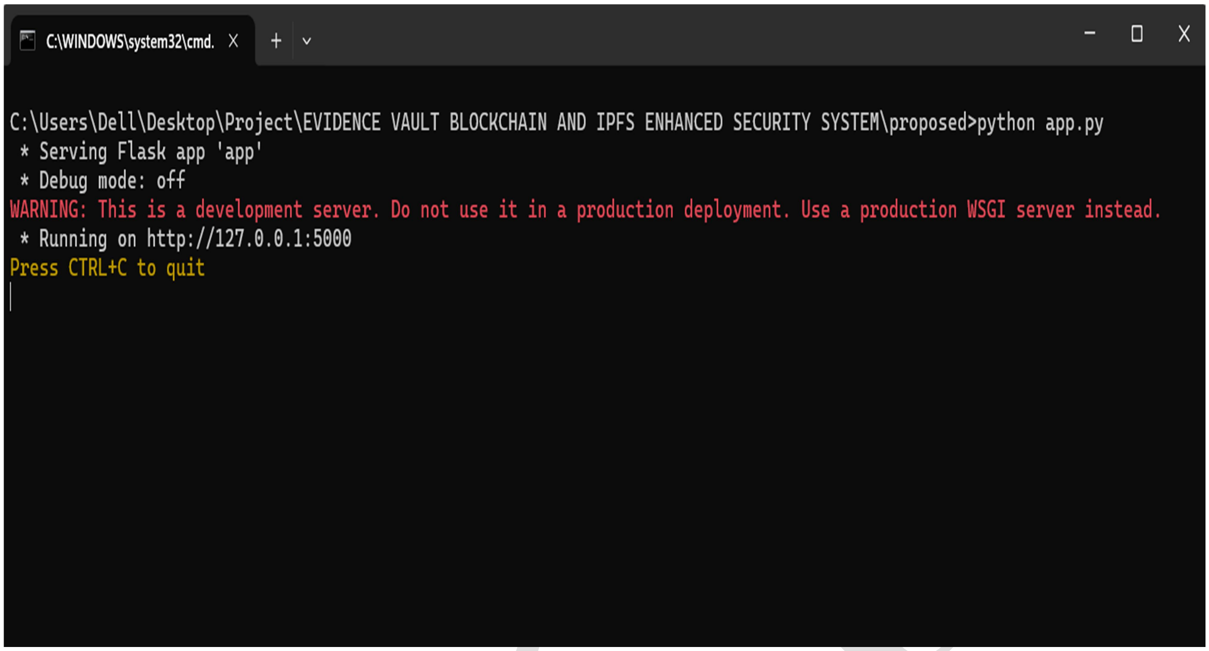
```
C:\Users\Dell\Desktop\Project\EVIDENCE VAULT BLOCKCHAIN AND IPFS ENHANCED SECURITY SYSTEM\proposed>truffle develop
Truffle Develop started at http://127.0.0.1:9545/

Accounts:
(0) 0x93242fac2b8bba8d284507ced887d2c30d6a3dd1
(1) 0xfa9ed31c7288bf2df20806889f018a2aba42af05
(2) 0x0026e83aacee74b74fcb2dee3facff636fc4f224
(3) 0xfcd0097abed7db219e35264e251f31478cc950ed
(4) 0x7648f23fbe9f2db8d785a474e1ad614f7443f9cb
(5) 0x53df504058e778c1dec3e1ffcb53e4cbe7b15e87
(6) 0x334ff8e31c2792287c2af5321b961095e70a4ecf
(7) 0x416c1dbb552bf7804a2de408900f5fd62eb285b5
(8) 0xed3cd2fe2a8a134812b601fb08ab1dca7ebfeaad
(9) 0xade44f940462b55af07474f615b9c9f2690d1dfc

Private Keys:
(0) 8b899e830170013a386d7c93e31493207f9b4e15fe924277962580bc6481037c
(1) d38340827f1fd31f91fa1cbe79b07a63d2e2e4d2810c745829130b8bb9d20a96
(2) e3daf51ee1051cae06ca279aacaaf527945447b329817aeadb88b39effa7c7be
(3) 7d89cf7ae6d951f8bec632cd7afc85581222495804b983c6c89da73e79181003
(4) 29790e5aec189bcf00b1f477d28efc37f5ddf73a312f5ab09f3cdebf1b9c1ba6
(5) 2dc412ff59ec840e14f2d937aac0bb286d6ceb8ce794cfa5bdfaa2c2f6efb477
(6) 4defd13727fe9079f36ab830e28537e4bde84e7b71a24e797e93e585e4a1406f
(7) 08c87b291e666c2df91ed88c1eda6bd9b1da199ee13dc09673836fb06fd33b93
(8) d2b860e72c8d7b55f3d9e76b265d346359a6603eb1d0ddc942963bb055a00598
(9) 160e12b5c3926afe1864adf9e8a6de2d3ceb9e2e96ff44538d93aae61b4e4898

Mnemonic: diamond tilt high logic melt torch element admit pave another torch quote
```

Fig. 7 Command Prompt installing Blockchain server with Private Keys.



```
   Replacing 'Evidence'
   --------------------

   > transaction hash:    0xa3519e01085d454c71a5e19d5aced1371c117f5749d3808be459355d2205bb74

   > Blocks: 0            Seconds: 0
   > contract address:    0xfA73CA2cE0C205066934D991aac5C05D95255f15
   > block number:        3
   > block timestamp:     1715143003
   > account:             0x93242FaC2B8bBa8d284507ced887d2c30d6a3DD1
   > balance:             99.996335063020154121
   > gas used:            844942 (0xce48e)
   > gas price:           3.178238866 gwei
   > value sent:          0 ETH
   > total cost:          0.002685427503915772 ETH


   > Saving migration to chain.

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.002685427503915772 ETH

Summary
=======
> Total deployments:   2
> Final cost:          0.003514654878915772 ETH
```

Fig. 8 Deployment of temporary Ethereum cryptocurrency and total cost of a transaction.



```
C:\Users\Dell\Desktop\Project\EVIDENCE VAULT BLOCKCHAIN AND IPFS ENHANCED SECURITY SYSTEM\proposed>python app.py
 * Serving Flask app 'app'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
```

Fig. 9 Deploying the frontend website with a temporary private address.

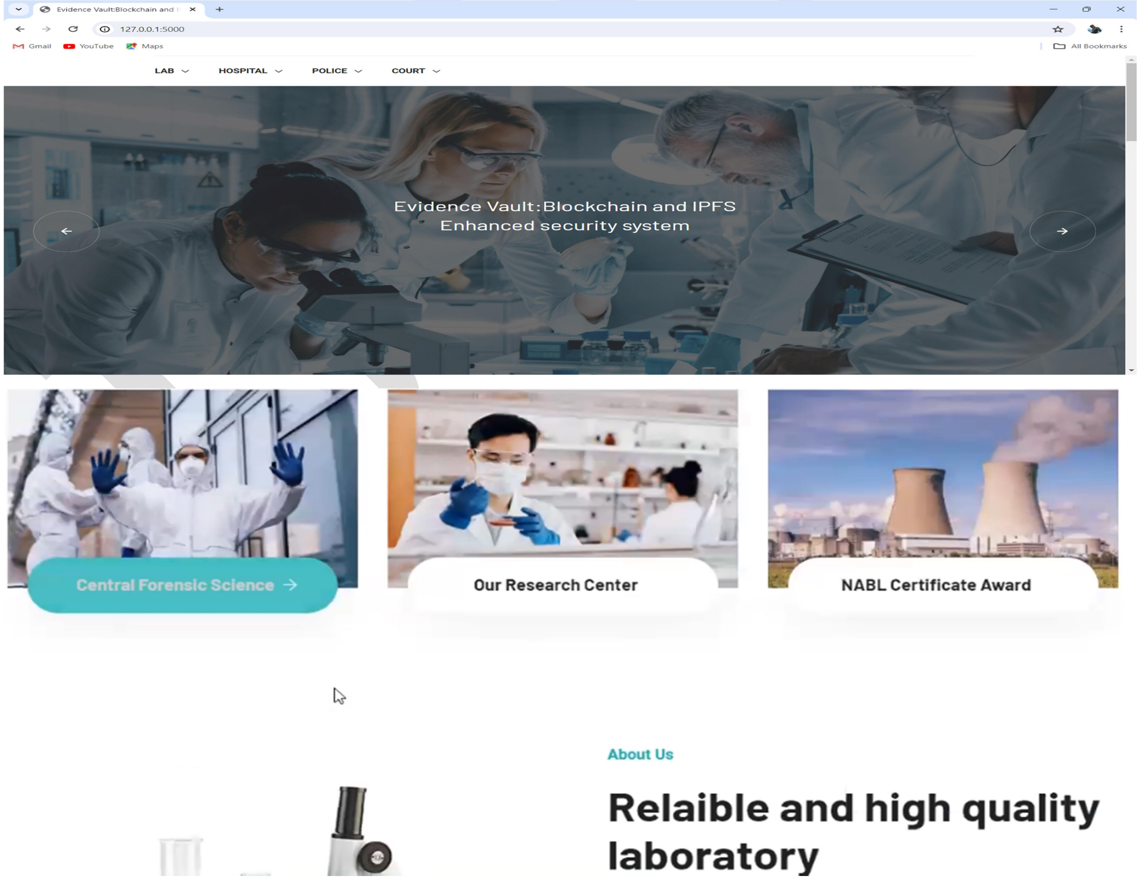
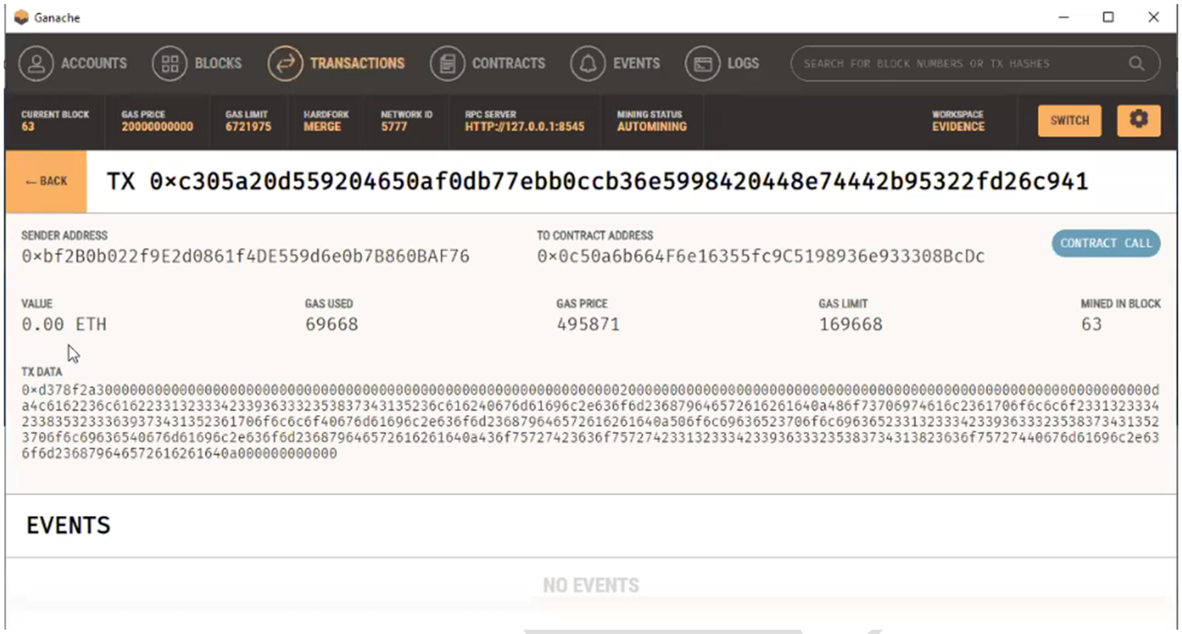


Fig. 10 Overview of the website of the Evidence Vault.



CURRENT BLOCK 63 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:8545 | MINING STATUS AUTOMINING | WORKSPACE EVIDENCE

TX 0×c305a20d559204650af0db77ebb0ccb36e5998420448e74442b95322fd26c941

SENDER ADDRESS
0×bf2B0b022f9E2d0861f4DE559d6e0b7B860BAF76

TO CONTRACT ADDRESS
0×0c50a6b664F6e16355fc9C5198936e933308BcDc

VALUE	GAS USED	GAS PRICE	GAS LIMIT	MINED IN BLOCK
0.00 ETH	69668	495871	169668	63

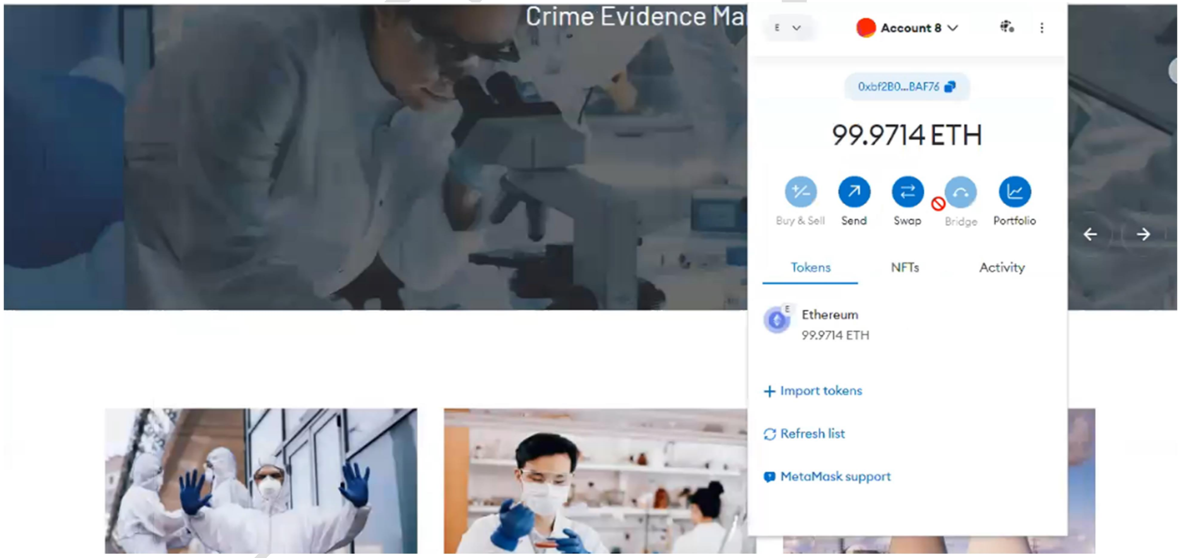
TX DATA

```
0×d378f2a300000000000000000000000000000000000000000000000000000000000000200000000000000000000000000000000000000000000000000000000000000d
a4c6162236c616223313233342339363332353837343135236c616240676d61696c2e636f6d236879646572616261640a486f73706974616c2361706f6c6c6f2331323334
23383532333639373431352361706f6c6c6f40676d61696c2e636f6d236879646572616261640a506f6c69636523706f6c696365233132333423393633323538373431352
3706f6c69636540676d61696c2e636f6d236879646572616261640a436f75727423636f7572742331323334233936333235383734313823636f75727440676d61696c2e63
6f6d236879646572616261640a000000000000
```

EVENTS

NO EVENTS

Fig. 11 Ganache application showing the record of transactions made.



99.9714 ETH

Ethereum
99.9714 ETH

Fig. 12 Meta Mask extension showing the Ethereum cryptocurrency balance.

CONCLUSION

Blockchain technology has improved the security of digitizing criminal evidence. The cryptographic features and unique hash codes provide a strong protection against tampering, guaranteeing the integrity of the data. This blockchain implementation preserved the integrity of the Chain of data by preserving the sequential arrangement of digital data. This feature offers investigators an unmodified and dependable sequence that is essential for maintaining the integrity of the investigation process. The use of blockchain enabled the decentralized and transparent sharing of digital evidence among all parties concerned. This not only improves productivity but also decreases dependence on a central authority, promoting a more flexible and cooperative investigative atmosphere. The use of smart contracts on the Ethereum blockchain enhanced the transparency of communication protocols. Trust is built in the system by establishing rules and assuring verifiable interactions, eliminating the need for third-party intermediaries and enhancing security and efficiency. The implementation of IPFS has been integrated to provide a safe and distributed storage system for evidence files. This enhances security by using content addressing and hash codes, which in turn ensures a storage solution that is resistant to tampering.

REFERENCES

[1] [1] Satoshi Nakamoto " Bitcoin: A peer_to_peer electronic Cash System," May 2008. (online). available: https://bitcoin.org/Bitcoin.pdf

[2] [2] Baygin, N., Baygin, M., & Karakose, M. (2019). Blockchain Technology: Applications, Benefits and Challenges. 2019 1st International Informatics and Software Engineering Conference (UBMYK).

[3] [3] V. Buterin," A next-generation smart contract and decentralized application platform, "White Paper,2014, Ethereum Foundations, Tech.Rep.2014[online].

[4] [4] Zibin Zheng Shaon Xie, "An overview of Blockchain Technology: Architecture, Consensus, and Future Trends",2017; IEEE 6th International Congress on Big Data.

[5] Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," *Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023

[6] Md. Zainlabuddin, "*Wearable sensor-based edge computing framework for cardiac arrhythmia detection and acute stroke prediction*", Journal of Sensor, Volume2023.

[7] Md. Zainlabuddin, "*Security Enhancement in Data Propagation for Wireless Network*", Journal of Sensor, ISSN: 2237-0722 Vol. 11 No. 4 (2021).

[8] Dr MD Zainlabuddin, "*CLUSTER BASED MOBILITY MANAGEMENT ALGORITHMS FOR WIRELESS MESH NETWORKS*", Journal of Research Administration, ISSN:1539-1590 | E-ISSN:2573-7104 , Vol. 5 No. 2, (2023)

[9] Vaishnavi Lakadaram, " Content Management of Website Using Full Stack Technologies", Industrial Engineering Journal, ISSN: 0970-2555 Volume 15 Issue 11 October 2022

[10] Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526

[11] Ijteba Sultana, Mohd Abdul Bari and Sanjay," *Impact of Intermediate per Nodes on the QoS Provision in Wireless Infrastructure less Networks*", Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021

[12] M.A.Bari, Sunjay Kalkal, Shahanawaj Ahamad," *A Comparative Study and Performance Analysis of Routing Algorithms*", in 3rd International Conference ICCIDM, Springer - 978-981-10-3874-7_3 Dec (2016)

[13] Mohammed Rahmat Ali,: BIOMETRIC: AN e-AUTHENTICATION SYSTEM TRENDS AND FUTURE APLLICATION", International Journal of Scientific Research in Engineering (IJSRE), Volume1, Issue 7, July 2017

[14] Mohammed Rahmat Ali,: BYOD.... A systematic approach for analyzing and visualizing the type of data and information breaches with cyber security", NEUROQUANTOLOGY, Volume20, Issue 15, November 2022

[15] Mohammed Rahmat Ali, Computer Forensics -An Introduction of New Face to the Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-453 – 456, Volume: 5 Issue: 7

[16] Mohammed Rahmat Ali, Digital Forensics and Artificial Intelligence ...A Study, International Journal of Innovative Science and Research Technology, ISSN:2456-2165, Volume: 5 Issue:12.

[17] Mohammed Rahmat Ali, Usage of Technology in Small and Medium Scale Business, International Journal of Advanced Research in Science & Technology (IJARST), ISSN:2581-9429, Volume: 7 Issue:1, July 2020.

[18] Mohammed Rahmat Ali, Internet of Things (IOT) Basics - An Introduction to the New Digital World, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169-32-36, Volume: 5 Issue: 10

[19] Mohammed Rahmat Ali, Internet of things (IOT) and information retrieval: an introduction, International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume: 7 Issue: 4, October 2017.

[20] Mohammed Rahmat Ali, How Internet of Things (IOT) Will Affect the Future - A Study, International Journal on Future Revolution in Computer Science & Communication Engineering, ISSN: 2454-424874 – 77, Volume: 3 Issue: 10, October 2017.

[21] Mohammed Rahmat Ali, ECO Friendly Advancements in computer Science Engineering and Technology, International Journal on Scientific Research in Engineering(IJSRE), Volume: 1 Issue: 1, January 2017

[22] Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay, "*Routing Quality of Service for Multipath Manets, International Journal of Intelligent Systems and Applications in Engineering"*, JISAE, ISSN:2147-6799, 2024, 12(5s), 08–16;

[23] Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46

[24] Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct : 021

[25] Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022

[26] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6

[27] .A.Bari& Shahanawaj Ahamad, "Managing Knowledge in Development of Agile Software", in International Journal of Advanced Computer Science & Applications (IJACSA), ISSN: 2156-5570, Vol: 2, No: 4, pp: 72-76, New York, U.S.A., April 2011

[28] Imreena Ali (Ph.D), Naila Fathima, Prof. P.V.Sudha ,"Deep Learning for Large-Scale Traffic-Sign Detection and Recognition", Journal of Chemical Health Risks, ISSN:2251-6727/ JCHR (2023) 13(3), 1238-1253

[29] Imreena, Mohammed Ahmed Hussain, Mohammed Waseem Akram" An Automatic Advisor for Refactoring Software Clones Based on Machine Learning", Mathematical Statistician and Engineering ApplicationsVol. 72 No. 1 (2023)

[30] Mrs Imreena Ali Rubeena,Qudsiya Fatima Fatimunisa "Pay as You Decrypt Using FEPOD Scheme and Blockchain", Mathematical Statistician and Engineering Applications: https://doi.org/10.17762/msea.v72i1.2369 Vol. 72 No. 1 (2023)

[31] Imreena Ali , Vishnuvardhan, B.Sudhakar," Proficient Caching Intended For Virtual Machines In Cloud Computing", International Journal Of Reviews On Recent Electronics And Computer Science , ISSN 2321-5461,IJRRECS/October 2013/Volume-1/Issue-6/1481-1486

[32] Heena Yasmin, A Systematic Approach for Authentic and Integrity of Dissemination Data in Networks by Using Secure DiDrip, INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES, Volume VI /Issue 5 / SEP 2016

[33] Heena Yasmin, Cyber-Attack Detection in a Network, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)

[34] Heena Yasmin, Emerging Continuous Integration Continuous Delivery (CI/CD) For Small Teams, Mathematical Statistician and Engineering Applications, ISSN:2094-0343, Vol.72 No.1(2023)