International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I8P212

Volume 71 Issue 8, 143-151, August 2023
© 2023 Seventh Sense Research Group®

Original Article

Forensic Evidence Security System using Blockchain Technology

Akinseye Oluwaseyitan Charles[1], Abiodun Oguntimilehin[2], Oniyide Alabi Bello[3]

[1,2,3]Department of Mathematical and Physical Sciences, Afe Babalola University, Ado Ekiti, Nigeria.

[1]Corresponding Author : akinseyeoc@pg.abuad.edu.ng

Received: 23 April 2023 Revised: 12 June 2023 Accepted: 22 July 2023 Published: 15 August 2023

Abstract *- When cybercrime is being investigated, digital evidence is crucial because it can be used to connect criminals to their victims. As digital evidence moves through the chain of custody at various levels of hierarchy during a criminal investigation, it is crucial to ensure its integrity, authenticity, and auditability. There is a need for a safe proof system which guarantees that case files containing forensic evidences are safe throughout the period of their handling and after. The system developed in this work, named Digital Threat Investigator, is built on Hyperledger Fabric, a permissioned network that requires authorization for all users. In order to effectively address privacy and confidentiality concerns, access control, channel permissions, and participant settings are important. Furthermore, the blockchain can be used to store and share data assets. The original forensic data is fragmented, stored in the cloud, and connected via the blockchain in the Digital Threat Investigator, while the usage history of the original data is also stored on the blockchain. For data access scalability and traceability, the two processes collaborate. Programming was done using WordPress, HTML, CSS and PHP. Results from the testing of the system showed that the latency decreased steadily as the number of nodes in the blockchain decreased. Results showed an increase from 150ms to 353ms as the number of nodes increased from 1 to 8. This system proved to be a workable tool that could aid digital forensics investigation and ensure the safe handling of forensic evidences.*

Keywords *- Blockchain**,** Cyber-crime, Forensic, Hierarchy, Hyperledger.*

1. Introduction

Our society is becoming increasingly digitized. This can be seen in the number of smartphones and computers coming onto the market. It is evident that this has led to easier business transactions, higher productivity, profitable management, and easier access to information [3]. A revolution in technology has been brought about by blockchain, which has attracted interest from stakeholders across various industries involving digital content and forensic evidence. When a transaction is made in the blockchain, it goes through a procedure called consensus mechanism, in which some participants come to an understanding to approve the transaction. Malicious entities might indulge in fraudulent activity to illegally access evidence. Security is a relatively crucial factor in ensuring dependable data transmission and the confidentiality of data from the security system to those authorized to access it. However, these technologies have their drawbacks, digital crime has increased, and nations have grappled with these challenges. It may not be possible to stop digital crimes completely; however, significant and useful improvements in digital crime prosecution, processing, and storage of digital crime evidence have been implemented, improving the crime investigation process [4].

A blockchain is an increasing list of records. Since the creation of Bitcoin in 2008, it has developed and expanded, having a greater impact on all fields and industries [29]. It is a method for documenting information on a blockchain [28]. The genesis block, the first block in a blockchain, only contains the hash value of blocks that come after it. The decentralized nature of the blockchain allows for retrieving manipulated data [24]. This permits data to be adequately verified, ensuring its correctness and purity [6]. Although the system can be amazingly complex, it can preserve digital evidence and make it increasingly accessible to investigators [10].

A series of blocks containing the ledger transaction comprise the blockchain technology [18]. It logs the transaction in a blockchain, which is a type of public ledger [25]. It is a distributed ledger that keeps track of transactions and stores values in multiple copies distributed among numerous participants [27]. Each new piece of data added to the ledger is logged on a network of nodes distributed across the ledger. The nodes must concur on whether or not to add new data to the blockchain each time it is changed or added to the system. The platform is starting to be used outside the financial industry, though [5]. When moving from one level of the hierarchy to another, there must be a guarantee of the integrity and authenticity of the digital evidence because it is crucial to solving crimes because it links individuals to their criminal activities [17]. If there are indications of a change in evidence, it may not be valuable when brought to court [22,23]. Detecting criminal activities is essential in the digital forensic investigation process [13]. Chain of Custody refers to the documentation of the forensic registration process. It contains all the important steps that the investigator takes to solve the crime [9]. This chain of custody aids the investigation by allowing the investigator to show where the crime was committed, who committed the crime, and what kind of tools or equipment were used.

To make the evidence tamper-proof and maintain its purity when presented in court, it is then uploaded to a blockchain [23]. The investigator examines the forensic copy to determine what information or data can be gleaned from it. Subsequently, all the information received is forwarded to the police along with the evidence [1]. However, the challenge with this system is that digital security and evidence integrity can be compromised. It is possible for evidence to be altered by an individual once the device is in police custody or for someone to hack into the investigator's computer system and change some of the evidence [32]. This leaves the current system open to attack and unsafe for proper forensic investigation. Faced with this challenge, blockchain technology has emerged as a possible solution [19].

2. Literature Review

Stuart Haber and W. Scott Stonetta produced the earliest research on what appeared to be a blockchain in 1991 [33]. They discussed the technology in a presented white paper, and the study concluded that "time-stamping could be widened to enhance the originality of documents for which the time of creation itself is not the critical issue." Later in 1992, they added Merkle Trees to the system to make it more effective by allowing multiple documents to be collected in a single block. The modern blockchain was created in 2008 by an unidentified person using the pseudonym Satoshi Nakamoto, sixteen years later. According to Nakamoto, the purpose of the blockchain was to house a public transaction ledger for the cryptocurrency Bitcoin on the blockchain [34]. The project's overall objective was to establish a decentralized digital currency that could be used to solve the double spending problem.

In building an effective digital crime investigation system, it is important that the actors develop trust in the process and for themselves. This is important as a lack of trust could result in the evidence being tampered with and subsequently made irrelevant in the investigative process. To do this, authors in [30] proposed a blockchain-based provenance process model for digital investigation in a cloud environment. Their main goal was to improve stakeholder interactions and trust in the investigation and handling of digital forensics, which would increase the process' credibility. Digital forensics, according to the researchers in [8], consists of four processes: identification, collection, organization, and presentation. The stages of digital forensics were similarly listed as identification, preservation, analysis, and presentation in the work done in. Utilizing scientific methods to locate, gather, arrange, and present evidence is a component of digital forensics [11]. The examination of the evidence and the analysis of the evidence are the two main steps in this stage. An in-depth examination of the data being used as evidence is done by the investigator during the evidence examination. Utilizing various forensic tools is another aspect of this inspection. These instruments are used to extract and filter the information pertinent to the investigation and interesting to the investigator [31]. In the analysis stage, events are reconstructed using the data gathered. The goal of the evidence analysis is to find any supporting documentation that will help the case from both a technical and legal standpoint.

Attacks on government platforms have been rampant since the invention of the internet. Government databases store huge amounts of data about citizens, and it is often a prey zone for hackers who are looking to lynch the information to use it for criminal purposes such as financial fraud. The researcher in [2] found a solution to this in his proposed system using blockchain. He proposed a system based on blockchain applying the Ethereum framework. The results of his work proved that blockchain was promising in putting a check to financially related fraud in e-governance, online product reviews and other online transactions ensuring integrity, trust, immutability and authenticity. The authors of [15] also suggested a system built on Ethereum, a digital forensic Blockchain platform. It was noted that the Ethereum-based system offered authenticity, integrity, and transparency for data gathered from numerous sources. Present systems allow for loss in transit of evidence, but a system is needed where the users can readily acquire information and be certain of the information's correctness when needed [16]. Chain of Custody (CoC) is the sequential record of the handling, management, transfer, and examination of tangible, digital, or electronic evidence [21].

Detection of criminal activity is pivotal in the digital forensic investigation process. A blockchain-based forensic investigation framework was developed in [12] with the intention of detecting criminal activity in the Internet of Things environment and gathering interactions from various Internet of Things entities. The proposed system had the potential to simulate interaction transactions, but it proved to be ineffective at gathering and analyzing large amounts of data. In the past, photos, videos, and documents were only available in their physical forms. If any of these items were ever used as evidence in a court of law, they had to be kept secure and only permitted access by designated individuals in a designated evidence room [7]. A blockchain network, a client side, and a certificate authority server make up the Hyperledger fabric. Additionally, peer membership data from the blockchain can be stored on the servers of the certification authority. Public and private digital keys and other keys can be created and distributed to maintain this system [5].

Researchers in [26] developed a system applying the decentralized nature of blockchain, which they called the Internet of Things forensic chain (IoTFC). In their paper titled "Blockchain-based Digital Forensic Investigation Framework in the Internet of Things and Social Systems," the proposed system was found to have strong distributed trust between examiners and evidential entities as well as good authenticity, immutability, and traceability. They discovered from their system that the IoTFC could boost examiners' and evidence items' trust by making the audit train transparent. A systematic literature review on blockchain for the Internet of Things was conducted by the authors of [7]. The use and adaptability of blockchain, specifically in relation to IoT and other peer-to-peer devices, were the focus of this study.

Interestingly, they stressed the possibility of detecting data abuse using the blockchain without needing a centralized reporting system. They did not, however, examine the broad implications of blockchain for overall cyber security. Bitcoin is a decentralized network allowing users to transact directives peer-to-peer, without a middle to manage the exchange of funds. It records transactions in a distributed ledger called blockchain [25].

Blockchain is a protocol that powers the Bitcoin network. Since then, the blockchain has developed into a distinct idea, and thousands of blockchains have been built using related cryptographic methods. Currently, Bitcoin wants to serve as both a store of value and a payment system. Although a consensus would need to be reached to add these systems to Bitcoin, there is nothing to say that it will not be used in this way in the future [18].

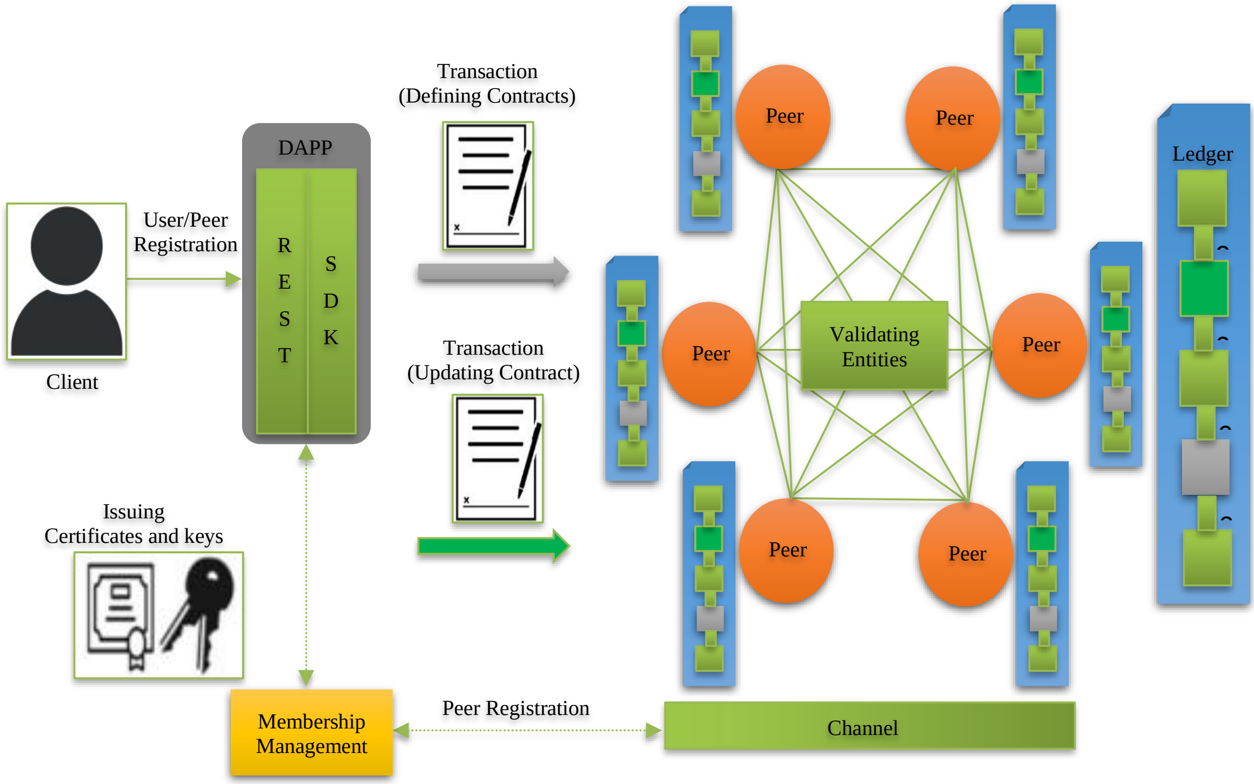
A distributed ledger program called Corda processes and stores data to support a network environment that is not centralized [14]. The Corda blockchain enables users to have multiple parties coexist within one network. The users will be able to interoperate with the same network system, in contrast to any type of permissioned blockchain network [31].

With Corda, users must come to a consensus in order for the entire virtual machine or entire ledger system to function. This distinguishes it from other blockchains. Any exchange between two parties will only be visible to those parties and no one else. But users who will participate in the consensus can also see them because they have to confirm it for the sake of the ledger [32]. Figure 1 shows the architecture of the hyperledger fabric framework.

3. Methodology

Related existing works in the field of securing forensic shreds of evidence were reviewed. Data was obtained from an online source, https://digitalcorpora.org. The designed system, called Digital Threat Investigator, is built on the Hyperledger Fabric platform, which supports permissioned networks in which each user is required to have their permissions granted. The forensic data management system can isolate various services in the blockchain network in accordance with user needs via the blockchain channel. Additionally, channels may be made private and limited to a particular group of users. To create permissions that are linked to particular organizations, a public key is used. In order to effectively address privacy and confidentiality concerns, access control, channel permissions, and participant settings are important.

Furthermore, the blockchain can be used to store and share data assets. The usage history of the original data is stored on the blockchain, and the authentic forensic information is dispersed, saved to the cloud, and linked via the blockchain. For data access scalability and traceability, the two processes collaborate. Programming was done using WordPress, HTML, CSS, and PHP. The system's development architecture is shown in Figure 2.



(Source: https://doi.org/10.3390/s21093051)

Fig. 1 Hyperledger fabric framework

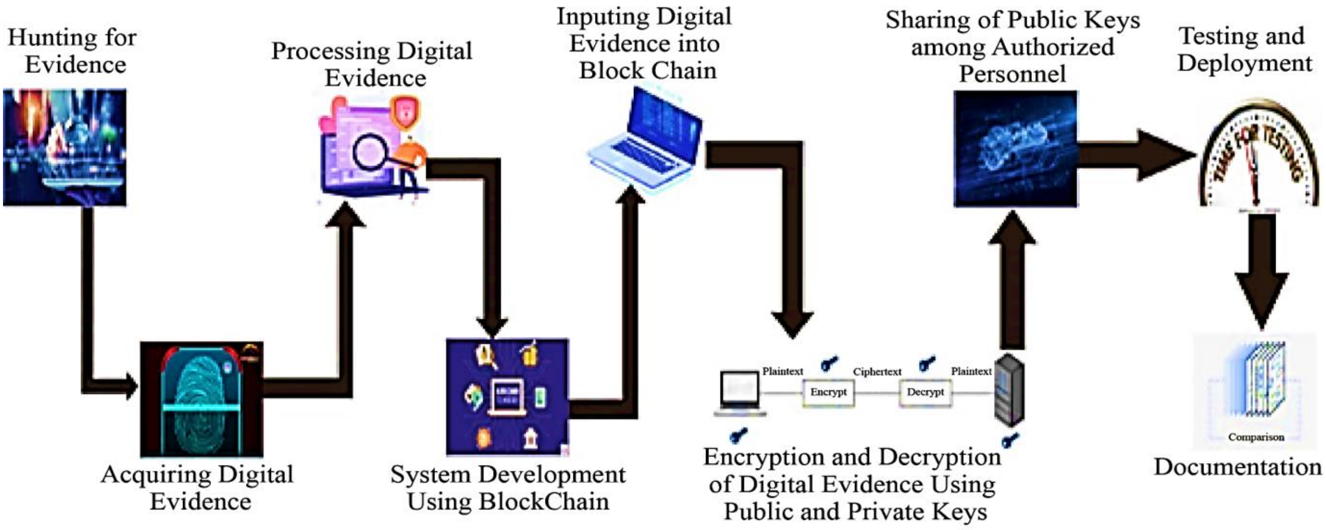

Hunting for Evidence
Processing Digital Evidence
Inputing Digital Evidence into Block Chain
Sharing of Public Keys among Authorized Personnel
Testing and Deployment
TIME FOR TESTING
Acquiring Digital Evidence
System Development Using BlockChain
Plaintext
Ciphertext
Plaintext
Encrypt
Decrypt
Encryption and Decryption of Digital Evidence Using Public and Private Keys
Comparison
Documentation

Fig. 2 System architecture

The system development process follows the architecture shown in Figure 2; the stages involved are discussed below:

3.1. Hunting for Evidences

When searching for evidence, a forensic investigator tries to find evidence from all possible sources, depending on the perpetrator and the crime committed [7]. Forensic evidence is captured from crime scenes using digital recording devices such as phones, digital cameras, etc. Forensic investigators are usually lawfully invited to crime scenes.

3.2. Capturing Evidence

When the forensic investigator sees the evidence, he captures the evidence. The different phases of the evidence-gathering process are:

Evidence Collection: It refers to collecting evidence at the crime scene. In this case, the investigator takes pictures and videos of the crime scene or the evidence site. To accomplish this, the investigator used a camera to capture images and/or video of the crime scene or crime scene.

Evidence Preservation: This is about labeling and storing the collected evidence in a well-protected environment. To accomplish this, the researcher appropriately labels each of the files and stores them in a well-labeled folder on a storage device.

3.3. System Development using Blockchain Technology

This digital evidence security system called Digital Threat Investigator (DTI) in this work was developed using blockchain technology based on Hyperledger Framework installed in a virtual and cloud-based Steem system and connected with a http/php user end.

3.4. Testing and Deployment

At this stage of the work, among other things, satisfaction, processing speed, confidentiality and other security requirements are analyzed. A replica of the actual production environment was set up using multiple distributed clients or loggers and the hyperbook scale client number option, deploying the system on a virtual and cloud-based system. Tests performed include: scalability, throughput and latency, and efficient storage capacity.

3.5. Encryption of Digital Evidence

A five-line of encrypting code was applied using the built-in basic encrypt( ) function applying Node JS in the hyperledger fabric framework for the encryption process of the Digital Threat Investigator. This encrypts ( ) function takes argument data with the predefined encryption password via environment variables (.env). An encryption key is created based on the aes256 algorithm, which encrypts data with the encryption key and returns the encrypted data. The codes are given thus:

```
Function encrypt(data){const cipher = crypto.createCipher('aes256', password);
let encrypted = cipher.update(data, 'utf8', 'hex'); encrypted += cipher.final('hex');return encrypted;}
```

3.6. Decryption of Digital Evidence

The Decryption process for this work involved another five lines of code using the hyperledger fabric's decrypt () function made available by Node JS. The decrypt() function decrypts the encrypted data. The decrypt() function again takes one argument— cipherData. The password creates a decryption key based on the aes256 algorithm and decrypts cipherData with the decryption key, and subsequently returns plain data. The codes are presented thus:

```
Function decrypt(cipherData) {const decipher = crypto.createDecipher('aes256', password);
  let decrypted = decipher.update(cipherData, 'hex', 'utf8');
decrypted += decipher.final('utf8');
  return decrypted.toString();}
```

3.7. Sharing of Encryption and Decryption Keys Amongst Users of the Application

A public key is a cryptographic key that can be shared with anyone and does not need to be kept in a secure location. Only the associated private key can decrypt messages that have been encrypted using the public key. The recipient uses a private key to decrypt a message encrypted with a public key. Only the private key that matches the public key used to encrypt the message can be used to decrypt it. Figure 3 depicts the authentication of public and private keys.

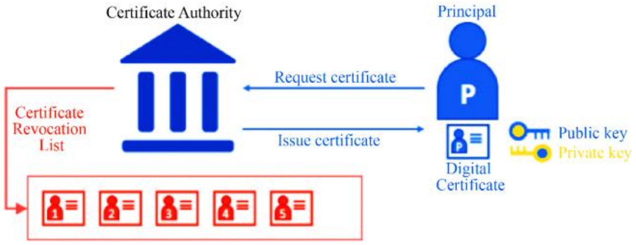


Fig. 3 Authentication process of public and private keys

4. Results and Discussion

4.1. Digital Threat Investigator: A Private Hyperledger Network

The system is a cloud-based blockchain system based on the Ubuntu 18.04 LTS virtual operating system on a Steam Cloud system. The virtual hard disk is very large because the system requires a lot of hard disk resources. The Digital Threat Researcher is built on top of the Hyperledger Fabric, which supports an authorized network where all participants must be authorized. The forensic data management system is able to isolate different services on the blockchain network in accordance with user needs through the blockchain channel. The machine is a cloud-primarily based totally blockchain machine constructed on a digital Ubuntu 18.04 LTS working machine on a Steam Cloud machine. The digital threat investigator is made to be very massive due to the machine requiring many difficult disk resources. It is primarily based totally on Hyperledger Fabric, which helps a permission community wherein all individuals ought to be authorized. Figure 4 depicts the installation of the hyperledger tools.

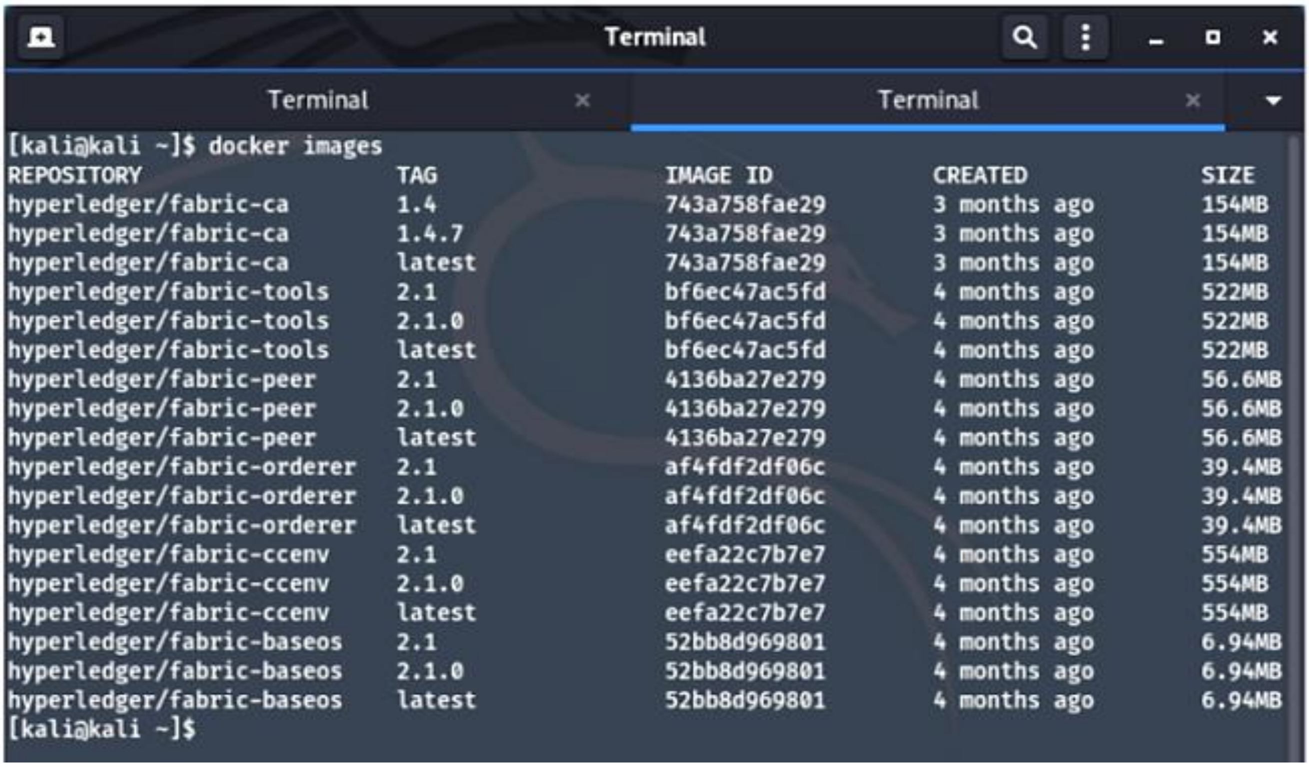
4.2. Developing the User Interface

As mentioned above, the user interface was developed using WordPress. This is due to the ease of development of the interface offered by WordPress and the possibility of connecting the blockchain system to it. Figure 5 displays the dashboard for the digital threat investigator platform.

4.3. Interface and Operation

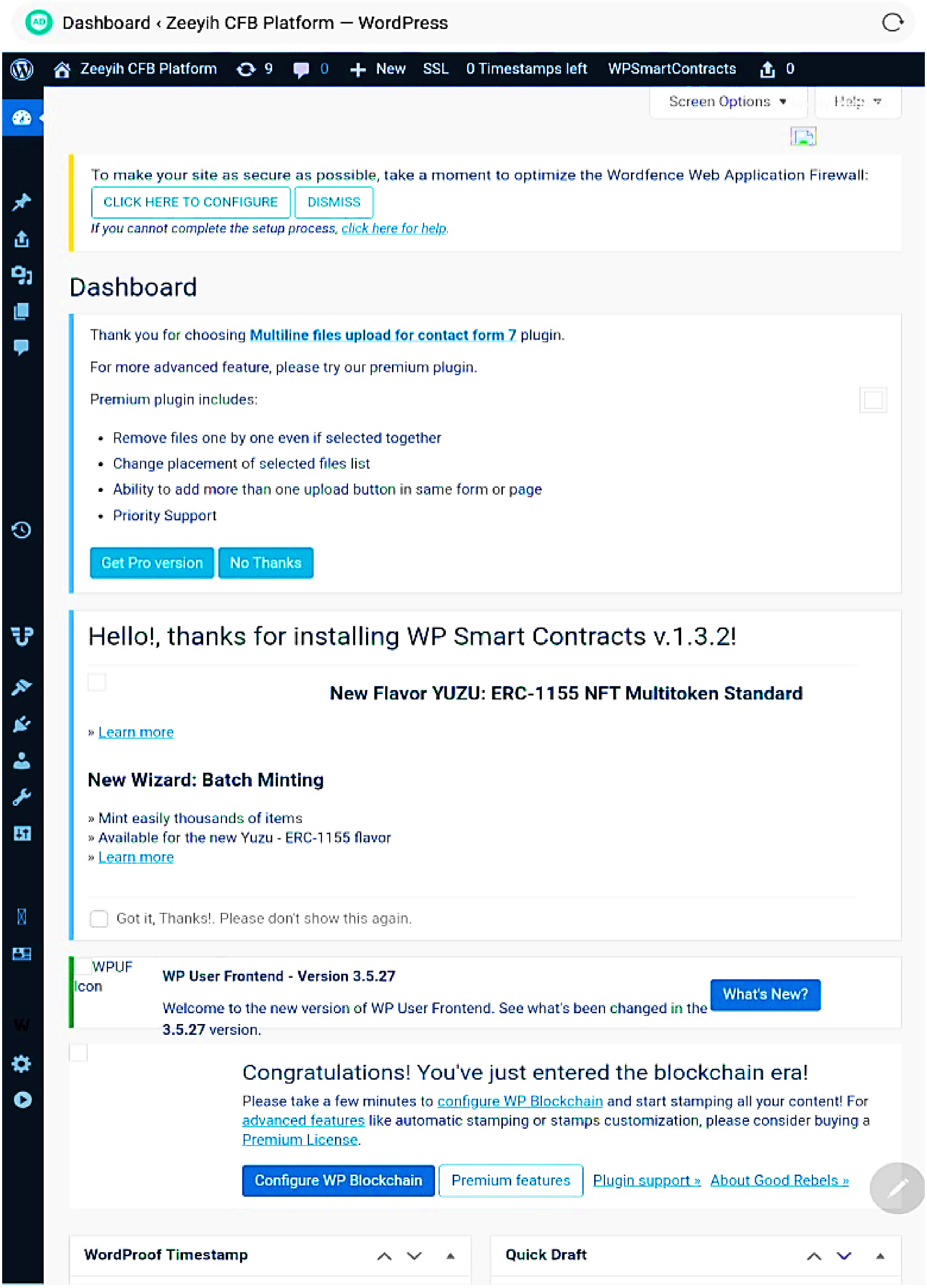
For digital forensic investigations, evidence review is performed by authenticated entities, ensuring privacy requirements are met. Because of this, only forensic evidence metadata is stored in Digital Threat Investigator, an approved distributed ledger built on Hyperledger Fabric on Steem. This represents an effort to offer audit and integrity services for the gathered evidence.

Digital evidence must have recorded information about the chronological history of its handling in order for involved parties to have access to it. Authenticated entities, also referred to as participants, have the ability to create blocks, issue new transactions, and claim ownership of forensic evidence. Figure 6 displays the Digital Threat Investigation Platform user interface.



```
[kali@kali ~]$ docker images
REPOSITORY                  TAG       IMAGE ID       CREATED        SIZE
hyperledger/fabric-ca       1.4       743a758fae29   3 months ago   154MB
hyperledger/fabric-ca       1.4.7     743a758fae29   3 months ago   154MB
hyperledger/fabric-ca       latest    743a758fae29   3 months ago   154MB
hyperledger/fabric-tools    2.1       bf6ec47ac5fd   4 months ago   522MB
hyperledger/fabric-tools    2.1.0     bf6ec47ac5fd   4 months ago   522MB
hyperledger/fabric-tools    latest    bf6ec47ac5fd   4 months ago   522MB
hyperledger/fabric-peer     2.1       4136ba27e279   4 months ago   56.6MB
hyperledger/fabric-peer     2.1.0     4136ba27e279   4 months ago   56.6MB
hyperledger/fabric-peer     latest    4136ba27e279   4 months ago   56.6MB
hyperledger/fabric-orderer  2.1       af4fdf2df06c   4 months ago   39.4MB
hyperledger/fabric-orderer  2.1.0     af4fdf2df06c   4 months ago   39.4MB
hyperledger/fabric-orderer  latest    af4fdf2df06c   4 months ago   39.4MB
hyperledger/fabric-ccenv    2.1       eefa22c7b7e7   4 months ago   554MB
hyperledger/fabric-ccenv    2.1.0     eefa22c7b7e7   4 months ago   554MB
hyperledger/fabric-ccenv    latest    eefa22c7b7e7   4 months ago   554MB
hyperledger/fabric-baseos   2.1       52bb8d969801   4 months ago   6.94MB
hyperledger/fabric-baseos   2.1.0     52bb8d969801   4 months ago   6.94MB
hyperledger/fabric-baseos   latest    52bb8d969801   4 months ago   6.94MB
[kali@kali ~]$
```

Fig. 4 Installation of the hyperledger tools



To make your site as secure as possible, take a moment to optimize the Wordfence Web Application Firewall:

If you cannot complete the setup process, click here for help.

Dashboard

Thank you for choosing **Multiline files upload for contact form 7** plugin.

For more advanced feature, please try our premium plugin.

Premium plugin includes:

- Remove files one by one even if selected together
- Change placement of selected files list
- Ability to add more than one upload button in same form or page
- Priority Support

Hello!, thanks for installing WP Smart Contracts v.1.3.2!

New Flavor YUZU: ERC-1155 NFT Multitoken Standard

» Learn more

New Wizard: Batch Minting

» Mint easily thousands of items
» Available for the new Yuzu - ERC-1155 flavor
» Learn more

□ Got it, Thanks!. Please don't show this again.

WP User Frontend - Version 3.5.27

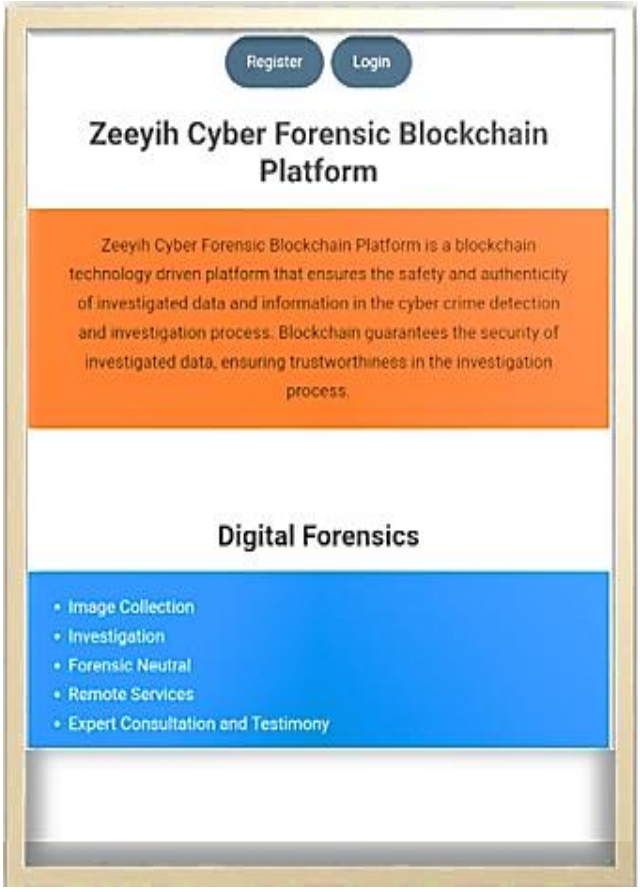
Welcome to the new version of WP User Frontend. See what's been changed in the 3.5.27 version.

Congratulations! You've just entered the blockchain era!

Please take a few minutes to configure WP Blockchain and start stamping all your content! For advanced features like automatic stamping or stamps customization, please consider buying a Premium License.

(Source: http://digitalthreatinvestigator.com.ng/dashboard/)

Fig. 5 Dashboard for the digital threat investigator platform



Register Login

Zeeyih Cyber Forensic Blockchain Platform

Zeeyih Cyber Forensic Blockchain Platform is a blockchain technology driven platform that ensures the safety and authenticity of investigated data and information in the cyber crime detection and investigation process. Blockchain guarantees the security of investigated data, ensuring trustworthiness in the investigation process.

Digital Forensics

- Image Collection
- Investigation
- Forensic Neutral
- Remote Services
- Expert Consultation and Testimony

Fig. 6 User interface for the digital threat investigator

4.4. Testing of the System

The chain/block ledger is filled first. This determines how the system behaves when large amounts of data are present in the system. The next step involved running a read-and-write transaction, where each transaction randomly reads and modifies the block. The system has been tried and tested to ensure forensic evidence is stored securely. The results of the system tests showed that latency steadily decreased as the number of nodes in the blockchain decreased. There was a reduction in latency from 270ms to 73ms. The performance results also showed an increase from 150 ms to 353 ms when the number of nodes increased from 1 to 8.

Figure 7 shows the latency graph of the blockchain system plotted by delay against several nodes. Figure 8 shows the graph of transaction throughput.

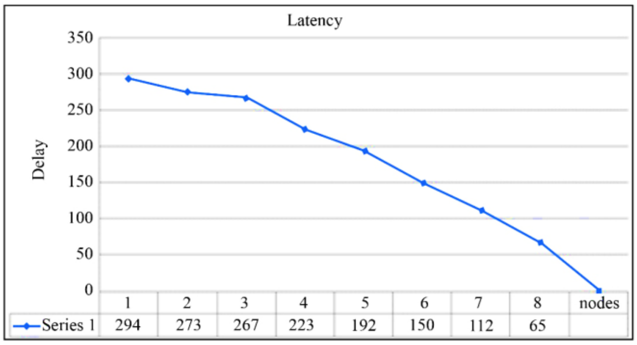


Fig. 7 Latency graph of the blockchain system plotted by delay against several nodes

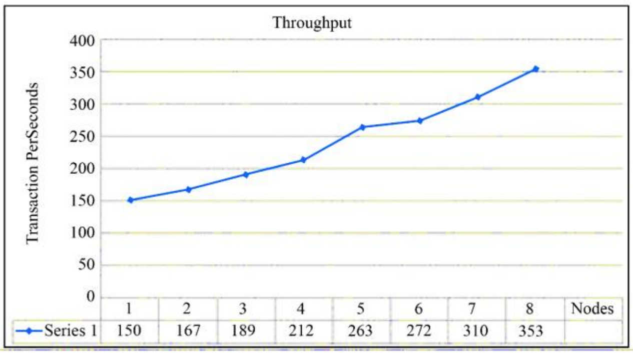


Fig. 8 Graph of transaction throughput

5. Conclusion

This study designed and developed a new Digital Forensic Investigation (DFI) model that included a digital blockchain to protect digital evidence's confidentiality, integrity, and authenticity. The results obtained showed that the Digital Threat Investigator model was able to fulfill the attributes of confidentiality, integrity and authenticity of the digital evidence.

Acknowledgment

The authors appreciate the Founder of Afe Babalola University for his financial support in the completion of this work.

References

[1] Luuc Van Der Horst, Kim-Kwang Raymond Choo, and Nhien-An Le-Khac, “Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core,” *IEEE Access*, vol. 5, pp. 22385–22398, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ameer Al-Nemrat, “Identity Theft on e-government/e-governance and Digital Forensics,” *International Symposium on Programming and Systems (ISPS)*, pp. 1–1, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Luca Caviglione, Steffen Wendzel, and Wojciech Mazurczyk, “The Future of Digital Supply Chain: Challenges and the Road Ahead,” *IEEE Security and Privacy*, vol. 15, no. 6, pp. 12-17, 2017. [CrossRef] [Publisher Link]

[4] Maxim Chernyshev et al., “Internet of Things Block Chain: The Need, Process Models, and Open Issues,” *IT Professional*, vol. 20, no. 3, pp. 40–49, 2018. [CrossRef] [Publisher Link]

[5] Mumin Cebe et al., “Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles,” *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50 – 57, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Lone, A. H., & Mir, R. N., “Forensic-Chain: Ethereum Blockchain based Digital Forensics Chain of Custody,” *Scientific & Practical Cyber Security Journal*, vol. 1, no. 2, pp. 21-27. 2018. [Google Scholar] [Publisher Link]

[7] Emmanuel Nyaletey et al., “BlockIPFS - Blockchain-Enabled Interplanetary File System for Supply chain and Trusted Data Traceability,” *IEEE International Conference on Blockchain (Blockchain),* pp. 18–25, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Larry E. Daniel, and Lars E. Daniel, *Digital Forensics for Legal Professionals, Understanding Digital Evidence from the Warrant to the Courtroom,* Elsevier, Syngress Book Co., 2012. [Google Scholar] [Publisher Link]

[9] Shancang Li et al., “Distributed Consensus Algorithm for Events Detection in Cyber-Physical Systems,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2299-2308, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Cheng Li, Liang-Jie Zhang, “A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things,” *IEEE International Congress on Internet of Things (ICIOT),* pp. 33–41, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ezz El-Din Hemdan, and D. H. Manjaiah, “CFIM : Toward Building New Cloud Forensics Investigation Model,” *Innovations in Electronics and Communication Engineering, Lecture Notes in Networks and Systems*, vol. 7, pp. 545–554, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mahmud Hossain, Yasser Karim, and Ragib Hasan, “FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger,” *IEEE International Congress on Internet of Things (ICIOT),* pp. 33–40, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ghita Mezzour et al., “A Socio-Computational Approach to Predicting Bioweapon Proliferation,” *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, pp. 458–467, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yang Liu, and Shiyan Hu, “Cyberthreat Analysis and Detection for Energy Theft in Social Networking of Smart Homes,” *IEEE Transactions on Computational Social Systems*, vol. 2, no. 4, pp. 148 – 158, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[15] Auqib Hamid Lone, and Roohie Naaz Mir, “Forensic-Chain: Ethereum Blockchain-Based Digital Forensics Chain of Custody,” *Scientific & Practical Cyber Security Journal*, pp. 21-27, 2017. [Google Scholar] [Publisher Link]

[16] Christopher S Meffert et al., “Forensic State Acquisition from Internet of Things (FSAIoT): A General Framework and Practical Approach for IoT Forensics through IoT Device State Acquisition,” *Proceedings of the 12th International Conference on Availability, Reliability and Security*, vol. 56, pp. 1-11, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[17] S. Li et al., "IoT Forensics: Amazon Echo as a Use Case," in *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6487-6497, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Ghita Mezzour et al., “A Socio-Computational Approach to Predicting Bioweapon Proliferation,” *IEEE Transactions on Computational Social Systems*, vol. 5, no. 2, pp. 458–467, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mahmud Hossain, Yasser Karim, and Ragib Hasan, “FIF-IoT: A Supply Chain Investigation Framework for IoT Using a Public Digital Ledger,” *IEEE International Congress on Internet of Things (ICIOT),* pp. 33–40, 2018. [CrossRef] [Publisher Link]

[20] T. Rajendran et al., “A Study on Blockchain Technologies for Security and Privacy Applications in a Network,” *SSRG International Journal of Electronics and Communication Engineering*, vol. 10, no. 6, pp. 69-91, 2023. [CrossRef] [Publisher Link]

[21] Shuai Wang et al., “Parallel Crime Scene Analysis Based on ACP Approach,” *IEEE Transactions on Computational Social Systems*, vol. 5, no. 1, pp. 244–255, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Ana Nieto, Rodrigo Roman, and Javier Lopez, “Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices,” *IEEE Network*, vol. 30, no. 6, pp. 34 – 41, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[23] Shancang Li, Li Da Xu, and Xinheng Wang, “Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 9, no. 4, pp. 2177–2186, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[24] Hubert Ritzdorf et al., “Toward Shared Ownership in the Cloud,” *IEEE Transactions on Information Blockchain and Security*, vol. 13, no. 12, pp. 3019–3034, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[25] Ankit Shah et al., “Understanding Tradeoffs between Throughput Quality and Cost of Alert Analysis in a CSOC,” *IEEE Transactions on Information Forensics Security*, vol. 14, no. 5, pp. 1155-1170, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[26] Shancang Li, Tao Qin, and Geyong Min, “Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems,” *IEEE Transactions on Computational Social Systems,* vol. 6, no. 6, pp. 1433-1441, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[27] Zhaoli Liu et al., “Behavior Rhythm: A New Model for Behavior Visualization and Its Application in System Security Management,” *IEEE Access,* vol. 6, pp. 73940–73951, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[28] Giannis Tziakouris, “Cryptocurrencies-A Forensic Challenge or Opportunity for Law Enforcement? An Interpol Perspective,” *IEEE Security Privacy*, vol. 16, no. 4, pp. 92-94, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[29] Abigail Paradise et al., “Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks,” *IEEE Transactions on Computational Social Systems*, vol. 4, no. 3, pp. 65-79, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[30] Yong Zhang et al., “A Blockchain-Based Process Provenance for Cloud Forensics,” *3rd IEEE International Conference on Computer and Communications (ICCC),* pp. 2470-2473, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[31] Shams Zawoad, Ragib Hasan, and Anthony Skjellum, “OCF: An Open Cloud Forensics Model for Reliable Digital Forensics,” *IEEE 8th International Conference on Cloud Computing*, pp. 437-444, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[32] Aleksandar Valjarevic, and Hein Venter, “A Harmonized Process Model for Digital Forensic Investigation Readiness,” *IFIP International Conference on Digital Forensics*, vol. 410, pp. 67-82, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[33] Stuart Haber, and W. Scott Stornetta, “How to Time-Stamp A Digital Document,” *Journal of Cryptology*, vol. 3, pp. 99-111, 1991. [CrossRef] [Google Scholar] [Publisher Link]

[34] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf