Uluslararası Sürdürülebilir Mühendislik ve Teknoloji Dergisi
International Journal of Sustainable Engineering and Technology
Sayı 2, Cilt 7, (2023), Sayfa: 131-138

PERFORMANCE COMPARISON OF SECURE STORAGE METHODS FOR DIGITAL FORENSIC EVIDENCE

Remzi GÜRFİDAN*[1], Muzaffer TATLI[1]

[1]Isparta Uygulamalı Bilimler Üniversitesi, Yalvaç Teknik Bilimler Meslek Yüksekokulu, Bilgisayar Programcılığı Bölümü, Isparta

Article Info
Received: 26.10.2023
Accepted:16.11.2023
Published:29.12.2023

ABSTACT

In the field of forensic informatics, digital data related to criminal and forensic investigations are collected, analysed, preserved and presented. Hacking, digital data recovery, data analysis, data analysis, data analysis, digital document analysis and analysis of data from mobile devices and other digital devices are included in the field of forensics. Using data collected from computers, mobile devices, hard disks, USB drives, digital cameras, cloud storage and other digital media, forensic experts are tasked with finding evidence. They also work on issues such as finding ways to protect against hackers and creating digital security measures. In a rapidly evolving digital world, the field of forensics is crucial for assisting criminal investigations and tracking the digital footprints of criminals. The guiding principles of forensic experts are legal compliance, accuracy, objectivity and security of evidence. During case analysis, law enforcement and prosecutors take photographs of the crime scene and evidence, after which the relevant report is written and the evidence file is created. The transparency and reliability of the procedure for the case in question is threatened by the vulnerability of this digitized and preserved content. Cyber-attacks that modify or destroy digital data result in the loss of relevant digital evidence. To prevent this problem and provide a solution, this paper compares the performance of a blockchain-based digital data storage application with a Tangle-based system. Photos of the incident environment and the incident report are combined and stored in the test model. The performance metrics of the system are rigorously measured. The study reveals that IOTA Tangle shows significant speed advantages (35 ms for 3KB images and 31 ms for 11KB images), especially in scenarios involving the storage of image data. In our analysis, Hyperledger Fabric performs commendably in character data processing, exhibiting lower response times (36 ms for 100 characters and 32 ms for 1000 characters) compared to IOTA Tangle.

Keywords; Digital Forensic, blockchain, data security, data privacy

DİJİTAL ADLİ DELİLLERİN GÜVENLİ DEPOLAMA YÖNTEMLERİNİN PERFORMANS KARŞILAŞTIRMASI

Makale Bilgisi
Geliş tarihi:26.10.2023
Kabul Tarihi:16.11.2023
Yayın tarihi:29.12.2023

ÖZET

Adli bilişim alanında, suç ve adli soruşturmalarla ilgili dijital veriler toplanır, analiz edilir, korunur ve sunulur. Hackleme, dijital veri kurtarma, veri analizi, veri analizi, dijital belge analizi ve mobil cihazlardan ve diğer dijital cihazlardan gelen verilerin analizi adli bilişim alanına dahildir. Bilgisayarlar, mobil cihazlar, sabit diskler, USB sürücüler, dijital kameralar, bulut depolama ve diğer dijital ortamlardan toplanan verileri kullanarak adli tıp uzmanları kanıt bulmakla görevlidir. Ayrıca bilgisayar korsanlarına karşı korunma yolları bulmak ve dijital güvenlik önlemleri oluşturmak gibi konular üzerinde de çalışırlar. Adli tıp alanı, hızla gelişen dijital dünyada cezai soruşturmalara yardımcı olmak ve suçluların dijital ayak izlerini takip etmek için çok önemlidir. Adli tıp uzmanlarının yol gösterici ilkeleri yasal uyumluluk, doğruluk, nesnellik ve kanıtların güvenliğidir. Vaka analizi sırasında kolluk kuvvetleri ve savcılar olay yeri ve delillerin fotoğraflarını çeker, ardından ilgili rapor yazılır ve delil dosyası oluşturulur. Söz konusu davaya ilişkin prosedürün şeffaflığı ve güvenilirliği, bu dijitalleştirilmiş ve korunmuş içeriğin savunmasızlığı nedeniyle tehdit altındadır. Dijital verileri değiştiren veya yok eden siber saldırılar, ilgili dijital kanıtların kaybolmasına neden olur. Bu sorunu önlemek ve bir çözüm sunmak için bu makale, blok zinciri tabanlı bir dijital veri depolama uygulamasının performansını Tangle tabanlı bir sistemle karşılaştırmaktadır. Olay ortamının fotoğrafları ve olay raporu birleştirilerek test modelinde saklanmaktadır. Sistemin performans metrikleri titizlikle ölçülmüştür. Çalışma, özellikle görüntü verilerinin depolanmasını içeren senaryolarda, IOTA Tangle'ın kayda değer hız avantajları (3KB görüntüler için 35 ms ve 11KB görüntüler için 31 ms) gösterdiğini ortaya koymaktadır. İncelememizde Hyperledger Fabric, karakter verilerinin işlenmesinde övgüye değer bir performans sergileyerek IOTA Tangle'a kıyasla daha düşük yanıt süreleri (100 karakter için 36 ms ve 1000 karakter için 32 ms) sergilemektedir.

Anahtar Kelimeler; Dijital Adli Tıp, blockchain, veri güvenliği, veri gizliliği

1. Introduction

Forensic informatics refers to the process of collecting, analysing and interpreting digital data that helps solve criminal cases or legal problems. Experts in this field contribute to legal processes by examining data transmitted or stored through computers, mobile phones, digital storage devices and other digital media (Çil and Demirci, 2022; Karie and Venter, 2015).

Forensic informatics experts collect data found at crime scenes or on suspects' digital devices. This is a critical step to obtain evidence or evidence of a crime. For example, emails, text messages or files deleted from a computer can be recovered by forensic experts and help solve the crime (Çil and Demirci, 2022). The collected data is analyzed and interpreted. This procedure helps to explain the suspects' behaviour or the way the crime was committed. Decoding concealed or encrypted data may be necessary for data analysis. Experts in forensic IT can provide testimony and exhibit digital evidence they have gathered and examined in court. Digital evidence can help identify a guilty or innocent person (Singh et al., 2023). Forensics is also used to protect computer systems and digital data (O'Malley, 2015). Detecting and closing security vulnerabilities provides defence against hackers or malicious software attacks. Forensics makes an important contribution to solving crimes and ensuring the rule of law. Due to the increasing number of crimes in the digital world and the role of digital data in legal processes, forensics has become an indispensable component in the legal systems of modern societies.

Maintaining confidentiality and integrity of information requires the storing of documents and information securely. Information integrity is well protected by blockchain technology. Every block is linked together and includes both its own content and the content of the block before it. Therefore, when it is necessary to modify a block to change or delete data, it will be necessary to modify all blocks (Ferrag and Shu, 2021). This makes it almost impossible to change or manipulate information. In addition, blockchain structures store information not on a centralized server, but distributed across a network. This reduces the risk of information being lost if a single point is attacked or fails. The blockchain cryptographically secures users' information (Halpin and Piekarska, 2017) and grants access to it only when necessary. This ensures better protection of documents and personal data. Blockchain networks generally offer high accessibility. This means that documents and information can be accessed at any time and from anywhere. Blockchain can be used to track when documents and information were created and who accessed them. This helps in meeting audit and traceability requirements. Data on the blockchain requires many approval processes before it can be modified. This makes it easy to verify the accuracy and validity of documents and information. Smart contracts on the blockchain enable documents to be managed automatically. For example, a document can automatically become invalid on a certain date, or documents that meet a set of conditions can be automatically approved. For these reasons, blockchain technology is considered a powerful tool for the secure storage of documents and information. Especially in finance (Patel et al., 2022), healthcare (Attaran, 2020), supply chain and many other industries, this technology sets new standards in document and information management and increases security.

Tangle is a system that is used as the underlying technology of the cryptocurrency IOTA and works differently from traditional blockchain technologies. Tangle uses a directed unrelated graph (DAG) structure (Gangwani et al., 2021; Hellani et al., 2021). This means that transactions are organized in a graph, not in a single chain. Each transaction is made to confirm two previous transactions that depend on it. In this way, transactions are interconnected on the network and form a graph instead of a chain. In Tangle, any user can make transactions using the network and has the responsibility to approve other transactions (Rochman et al., 2023). When a transaction is submitted, users who wish to confirm it contribute to the network by validating the transaction and adding their own transactions. Transaction fees in Tangle are non-existent or very low. This is because the confirmation and verification of transactions is done by users and therefore there is no need to pay miners (Silvano and Marcelino, 2020).

In this study, the results obtained will be presented by comparing the limited performance measurements of IOTA Tangle and Hyperledger Fabric blockchain structure in storing evidence files. To implement these business processes, an IOTA Tangle and Hyperledger Fabric structure was prepared and measured.

2. Related Works

A blockchain-based digital forensics framework for Internet of Things environments is presented by Ryu et al. in their work. The suggested framework makes the current chain of custody procedure simpler and more effective by storing all IoT (Internet of Things) device connections as blockchain transactions. Blockchain technology ensures the integrity of the data to be studied, strengthens security, and improves the reliability of integrity protection through a decentralized integrity protection mechanism. Furthermore, participants in the forensic investigation, including device users, makers, investigators, and service providers, can transparently follow the investigation process because of the distributed ledger structure (Ryu et al., 2019). Li et al. conducted an analysis of the security and privacy risks associated with digital forensics legal evidence management. Based on their findings, they developed a legal evidence management system known as LEChain. The whole evidence flow in LEChain, from collection to review, analysis, and reporting, is driven by data. Legal organizations can more easily upload and retrieve pertinent data on the blockchain with LEChain, preventing dishonest police investigators from fabricating evidence. Both judges and witnesses are free to engage in the system. Ultimately, in order to assess the viability and effectiveness of the suggested plan, they put it into practice on the public network in Europe (M. Li et al., 2021). Kumar et al. put up a solution in their study for Internet of Things digital forensics applications. This work tests a novel approach to supplying security features on the blockchain: the usage of Programmable Hash Functions (PHFs). Along with the use of consortium blockchain for cross-border forensic data, a chain of custody solution is also taken into consideration. The application of smart contracts is used to gather forensic data. Edge computing includes embedded forensic applications, particularly at the fog layer that makes use of processing power. In addition to failure areas being found, the framework was assessed based on latency, throughput, gas consumption, energy and resource utilization (Kumar et al., 2021). Li et al. present a unique blockchain-based DF investigation framework that may offer privacy protection and proof-of-existence for the inspection of evidence items in the context of social systems and the Internet of Things. They provide the IoT forensic chain (IoTFC), a block-enabled forensics framework for IoT that may provide forensic investigation with good authenticity, immutability, traceability, flexibility, and distributed trust among auditors with rights of evidence, in order to implement these features. IoTFC can track the provenance of evidence items and provide traceability guarantees. Blockchains record the identification, preservation, analysis, and presentation of evidence. Because IoTFC makes the audit sequence transparent, it boosts the trust of both auditors and evidence items (S. Li et al., 2019). Forensic Chain: A Blockchain-Based Digital Forensics Chain of Custody is a study by Lone and Mir. The performance of the Hyperledger Composer-based Forensic Chain model prototype is assessed and provided. According to Lone and Mir (2019), the prototype showed a manageable overhead in terms of throughput and resource consumption with room for optimization for a full-scale end-to-end implementation. A safe and anonymous blockchain-based VDF method is proposed by Li et al. With decentralized anonymous credentials and no reliance on third parties, it seeks to safeguard privacy. Data providers upload vehicle information and supporting documentation to the blockchain, where they are kept in the distributed data store. Every inquiry is represented as a finite state machine, with smart contracts handling state transitions. Eunomia offers fine-grained evidence access management via Bulletproofs and ciphertext policy attribute-based encryption (M. Li et al., 2023). Gangwani and colleagues present the Tangle model, which leverages algorithms to analyse vast quantities of data and enable the development of a digital on-demand environmental ecosystem. This data is distributed, authenticated, and unchangeable. They have shown how encrypted environmental sensor data may be published and stored using the MAM protocol. To demonstrate the data's confidentiality, security, and integrity, IOTA Tangle is supplied (Gangwani et al., 2021). We offer in this study the first theoretical modelling, based on stochastic analysis, for the growing IOTA network. The main conclusions drawn from the analysis of real-world IOTA ledger data snapshots indicate that the degree distribution of the IOTA network is a very anomalous double Pareto Lognormal (dPLN). On the other hand, standard exponential and power law distributions are not true to reality. Using official data from the IOTA Foundation, we assess the suggested model and fitting algorithm (Guo et al., 2022). Rawat and colleagues conducted an experimental analysis of the IOTA specification concerning offline blockchain operations. The offline Tangle scenario was used to examine how the use edge selection algorithm affected offline transactions, including situations like the solidification effect and incomplete synchronization. The findings indicate that some nodes (public IOTA nodes) cannot be accessed by the coordinator. Temporal performance was also found to be faster than the standard blockchain structure (Rawat et al., 2022). Singh et al. propose a model for secure storage of digital evidence captured pre- and post-incident to achieve reactive forensics. Various components such as integrity checks, media sandboxing, strong encryption, two-factor authentication and unique random file naming are considered (Singh et al., 2022). Shobana et al. analyse the various methodologies currently in place for remote forensic investigation. Different state-of-the-art software and hardware tools and techniques are compared to perform different stages of the investigation. Comparison tables are presented to understand the advantages, disadvantages, challenges and opportunities involved in these techniques. The overall objective of this paper is to conduct comparative analysis based on qualitative outputs observed from memory, timeline and live forensic imaging in an incident that can simplify the process of finding the more appropriate technique under changing circumstances for effective remote forensic investigation.

3. Proposed Model

In the method proposed in this study, the report prepared by the user is converted into uft8 form and sent to the IOTA Tangle HORNET platform. The data sent to this platform is converted into Tangle structure and added to the line. Figure 1 shows the general architecture of the proposed evidence storage structure. The configuration of the nodes on the IOTA Tangle framework and the settings of the REST API to be used for transactions are realized in json format as follows.

```
"bindAddress": "0.0.0.0:14265",
      "powEnabled": true,
      "powWorkerCount": 1,
      "limits": {
         "bodyLength": "1M",
         "maxResults": 1000
```

bindAddress represents the IP and Port information that we will send data to the Tangle structure. The IP address 0.0.0.0 means that requests can be made from all IP addresses of the server where Tangle is running. The part after the ":" sign next to the IP address shows the port information. Client communications are made through this port. powEnabled controls whether the node does PoW when receiving messages through the API. powWorkerCount determines the number of workers used to calculate PoW when broadcasting messages through the API. bodyLenght indicates the maximum number of characters that the body of an API call can contain. maxResults indicates the maximum number of results that can be returned by an endpoint.

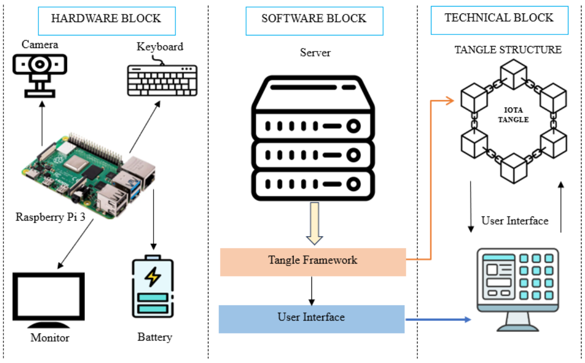


Figure 1. Architecture of the prepared digital evidence storage structure

Solid, unsolid, referenced, conflicting, milestone, unknown and type definitions are used to determine the nature of the data added on this platform and the nature of each node created. Solid confirms the soundness, correctness and validity of an operation performed in Tangle. Unsolid means that the operation is not sound or does not have sufficient validation. Referenced indicates that successive transactions are connected and validate each other. Conflicting Tangle refers to a situation where a transaction conflicts with the same source transaction or where different devices are trying to perform different operations on the same source. Milestone refers to transactions that are established at certain time intervals, used to increase the security of the network and to mark strong transactions. Unknown refers to transactions in Tangle that have not yet been verified and whose validity status is unknown. Type is used to specify transaction types such as data transfer, value transfer or private transaction.

The connection view of the data added on the IOTA Tangle framework in the interface is shown in Figure 2. The non-linear connections between nodes and node properties are clearly visible. The computer specifications on which the tests were performed are 8 core Intel processors and 16 GB RAM.

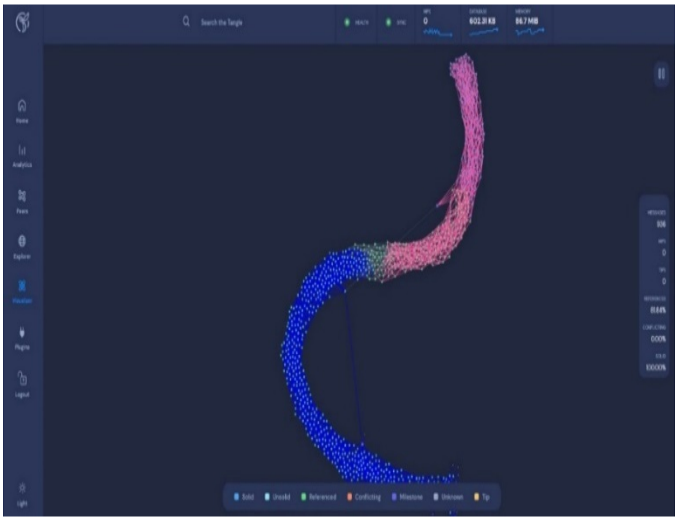
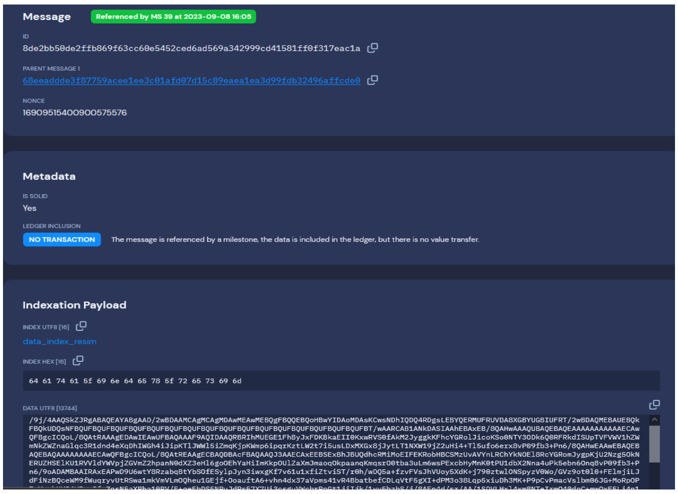


Figure 2. Connection view of the data added on the IOTA Tangle framework in the interface.

Figure 3 shows the details of a node added to the IOTA Tangle structure. In these details, Id, Nonce value, UTF-8 format of the data can be seen.



Message Referenced by MS 39 at 2023-09-08 16:05

ID
8de2bb50de2ffb869f63cc60e5452ced6ad569a342999cd41581ff0f317eac1a

PARENT MESSAGE 1
68eeaddde3f87759acee1ee3c01afd07d15c89eaea1ea3d99fdb32496affcde0

NONCE
16909515400900575576

Metadata

IS SOLID
Yes

LEDGER INCLUSION
NO TRANSACTION The message is referenced by a milestone, the data is included in the ledger, but there is no value transfer.

Indexation Payload

INDEX UTF8 [16]
data_index_resim

INDEX HEX [16]
64 61 74 61 5f 69 6e 64 65 78 5f 72 65 73 69 6d

DATA UTF8 [13744]

/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAMCAgMCAgMDAwMEAwMEBQgFBQQEBQoHBwYIDAoMDAsKCwsNDhIQDQ4RDgsLEBYQERMUFRUVDA8XGBYUGBIUFRT/2wBDAQMEBAUEBQk
FBQkUDQsNFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBT/wAARCAB1ANkDASIAAhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAw
QFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3ODk6Q0RFRkdISUpTVFVWV1hZW
mNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEB
AQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkN
ERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+P
n6/9oADAMBAAIRAxEAPwD9U6wtY8RzabqBtYbSOfESylpJyn3iwxgKf7v61u1xfiZtviST/r0h/wDQ5a+fzvFVsJhVUoy5XdK+j790ztwlONSpyzV0Wo/GVz9ot0l0+FElmjiLJ
dFiNzBQceWM9fWuqryvUtRSwa1mkVmVLmOQheu1GEjf+OoauftA6+vhn4dx37aVpms41vR4BbatbefCDLqVtF5gXI+dPM3o38Lqp5xiuDh3MK+P9pCvPPmacVslbm06JG+MoRpOP

Figure 3. Detail information of a node added to the IOTA Tangle structure.

We measured the time taken for data insertion and retrieval operations of different sizes and types on Hyperledger Fabric and IOTA Tangel Hornet platform. The results are shown in Table 1. When the performances are compared, it is seen that the performance of both platforms is very close to each other. IOTA Tangle is found to be slightly ahead in the processing of image data and slightly behind in the processing of character data.

Table 1. Performance of IOTA Tangle and Hyperledger Fabric for different data.

Transaction Data	IOTA Tangle	Hyperledger Fabric
Image (3Kb)	35 ms	38 ms
Image (11Kb)	31 ms	40 ms
100 characters	41 ms	36 ms
1000 character	59 ms	32 ms

First, it's critical to comprehend the primary distinctions between Hyperledger Fabric and IOTA Tangle. A graph, or tangle, is used by IOTA Tangle, a distributed ledger technology, in place of a collection of linked blocks. An open source blockchain architecture called Hyperledger Fabric was created especially for private blockchain applications in a variety of commercial settings and sectors. IOTA Tangle appears to respond more quickly than Hyperledger Fabric when it comes to image data with sizes of 3KB and 11KB. This suggests that the IOTA Tangle might work better with some kinds of data than others. For character data (100 and 1000 characters), the circumstances are different. On datasets with 100 and 1000 characters, Hyperledger Fabric displays slower reaction times, suggesting that Hyperledger Fabric could process this kind of data more quickly.

It can be stated that IOTA Tangle should be the appropriate infrastructure for the system in question given that the number of nodes in the Tangle structure increases and the transaction verification times speed up.

4. Conclusions

This study compares the performance of two well-known distributed ledger platforms, IOTA Tangle and Hyperledger Fabric, in order to evaluate the architecture of a digital evidence storage system. In forensic investigations, digital evidence is essential, and the effectiveness of the storage system that is used can have a big influence on the investigation's outcome. This evaluation considers the speed of transaction processing as a key metric, given its crucial role in handling digital evidence. One of the focal points of our investigation is the IOTA Tangle, a distributed ledger technology that utilizes a unique directed acyclic graph (DAG) structure. IOTA's reliance on previous transactions for the confirmation of new transactions is a distinguishing feature that can potentially enhance scalability. The study reveals that, especially in scenarios involving the storage of image data, IOTA Tangle demonstrates notable speed advantages (35 ms for 3KB and 31 ms for 11KB images). On the other hand, Hyperledger Fabric, designed specifically for enterprise use, stands out for its robust security features and sophisticated permission controls. This makes it particularly suitable for applications with stringent privacy requirements. In our examination, Hyperledger Fabric exhibits commendable performance in handling character data, showcasing lower response times (36 ms for 100 characters and 32 ms for 1000 characters) compared to IOTA Tangle.

As we delve into the advantages and disadvantages of these platforms, it becomes evident that IOTA Tangle excels in speed, especially for certain types of data, while Hyperledger Fabric prioritizes enterprise-grade security. IOTA's scalability through its unique confirmation mechanism could make it a preferred choice for applications where rapid transaction confirmation is crucial. Hyperledger Fabric, with its emphasis on security and permission controls, is well-suited for environments demanding strict access controls and data privacy.

In conclusion, the choice between IOTA Tangle and Hyperledger Fabric for storing digital evidence depends on the specific requirements of the use case. Balancing the need for speed with the imperative for robust security is paramount in the design process. Both platforms offer distinct advantages, and the decision should be guided by the nature of the digital evidence, the scalability requirements, and the privacy and security considerations of the application. As the landscape of distributed ledger technologies evolves, ongoing assessment and consideration of these factors will be crucial in optimizing the design of systems for storing digital evidence. Future studies aim to evaluate the effects of more distributed ledger technologies, especially rapidly developing technologies in this field, on digital evidence storage systems. By expanding performance comparisons between different platforms, the ultimate goal is to gain a more detailed understanding of performance across various scenarios and data types.

References

Attaran, M., 2020. Blockchain technology in healthcare: Challenges and opportunities. Https://Doi.Org/10.1080/20479700.2020.1843887, 15(1), 70–83. https://doi.org/10.1080/20479700.2020.1843887

Çil, A., and Demirci, M., 2022. Ağ Adli Bilişimi Süreç Gereksinimlerinin Belirlenmesi ve Yazılım Tanımlı Ağlarda İncelenmesi. Journal of Polytechnic, 1(1). https://doi.org/10.2339/politeknik.1141107

Çil, A., and Demirci, M., 2022. Determination of Network Forensics Process Requirements and Analysis in Software-Defined Networks. Journal Of Polytechnic-Politeknik Dergisi. https://doi.org/10.2339/POLITEKNIK.1141107

Ferrag, M. A., and Shu, L., 2021. The Performance Evaluation of Blockchain-Based Security and Privacy Systems for the Internet of Things: A Tutorial. IEEE Internet of Things Journal, 8(24), 17236–17260. https://doi.org/10.1109/JIOT.2021.3078072

Gangwani, P., Perez-Pons, A., Bhardwaj, T., Upadhyay, H., Joshi, S., and Lagos, L., 2021. Securing Environmental IoT Data Using

Masked Authentication Messaging Protocol in a DAG-Based Blockchain: IOTA Tangle. Future Internet 2021, 13(12), 312. https://doi.org/10.3390/FI13120312

Guo, F., Xiao, X., Hecker, A., and Dustdar, S., 2022. A Theoretical Model Characterizing Tangle Evolution in IOTA Blockchain Network. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2022.3207513

Halpin, H., and Piekarska, M., 2017. Introduction to security and privacy on the blockchain. Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017, 1–3. https://doi.org/10.1109/EUROSPW.2017.43

Hellani, H., Sliman, L., Samhat, A. E., and Exposito, E., 2021. Tangle the Blockchain: Towards Connecting Blockchain and DAG. Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE, 2021-October, 63–68. https://doi.org/10.1109/WETICE53228.2021.00023

Karie, N. M., and Venter, H. S., 2015. Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, 60(4), 885–893. https://doi.org/10.1111/1556-4029.12809

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

Li, M., Chen, Y., Lal, C., Conti, M., Alazab, M., and Hu, D., 2023. Eunomia: Anonymous and Secure Vehicular Digital Forensics Based on Blockchain. IEEE Transactions on Dependable and Secure Computing, 20(1), 225–241. https://doi.org/10.1109/TDSC.2021.3130583

Li, M., Lal, C., Conti, M., and Hu, D., 2021. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Generation Computer Systems, 115, 406–420. https://doi.org/10.1016/J.FUTURE.2020.09.038

Li, S., Qin, T., and 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. https://doi.org/10.1109/TCSS.2019.2927431

Lone, A. H., and Mir, R. N., 2019. Forensic chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44–55. https://doi.org/10.1016/J.DIIN.2019.01.002

O'Malley, T., 2015. Forensic informatics enabling forensic intelligence. Australian Journal of Forensic Sciences, 47(1), 27–35. https://doi.org/10.1080/00450618.2014.922618

Patel, R., Migliavacca, M., and Oriani, M. E., 2022. Blockchain in banking and finance: A bibliometric review. Research in International Business and Finance, 62, 101718. https://doi.org/10.1016/J.RIBAF.2022.101718

Rawat, A., Daza, V., and Signorini, M., 2022. Offline Scaling of IoT Devices in IOTA Blockchain. Sensors 2022, Vol. 22, Page 1411, 22(4), 1411. https://doi.org/10.3390/S22041411

Rochman, S., Istiyanto, J. E., Dharmawan, A., Handika, V., and Purnama, S. R., 2023. Optimization of tips selection on the IOTA tangle for securing blockchain-based IoT transactions. Procedia Computer Science, 216, 230–236. https://doi.org/10.1016/J.PROCS.2022.12.131

Ryu, J. H., Sharma, P. K., Jo, J. H., and Park, J. H., 2019. A blockchain-based decentralized efficient investigation framework for IoT digital forensics. Journal of Supercomputing, 75(8), 4372–4387. https://doi.org/10.1007/S11227-019-02779-9/FIGURES/7

Silvano, W. F., and Marcelino, R., 2020. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. Future Generation Computer Systems, 112, 307–319.

https://doi.org/10.1016/J.FUTURE.2020.05.047

Singh, A., Singh, N., Singh, S. K., and Nayak, S. K., 2023. Cyber-Crime and Digital Forensics: Challenges Resolution. 2023 International Conference on Computer Communication and Informatics, ICCCI 2023. https://doi.org/10.1109/ICCCI56745.2023.10128333

Singh, A., Ikuesan, R. A., and Venter, H., 2022. Secure storage model for digital forensic readiness. IEEE Access, 10, 19469-19480.

Shobana, G., 2021. The State of the art tools and techniques for remote digital forensic investigations. In 2021 3rd International Conference on Signal Processing and Communication (ICPSC). May 2021. 464-468. IEEE.