https://doi.org/10.48047/AFJBS.6.12.2024.4957-4968

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Securing IOT Applications with Kriper Blockchain: Enhancing Data Integrity and Security in Corporate World

Srinivasa Reddy Donthireddy[1], Nayeem Basha Shaik[2], Harsha Vardhan Paidipati[3], G. Bindu[4], Naga Venkata Karthikeya Madda[5]

[1]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. 2100030135cseh@gmail.com*

[2]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. 2100031115cseh@gmail.com*

[3]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. 2100030392cseh@gmail.com*

[4]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. bindugarikapati7@kluniversity.in*

[5]*Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. 2100030309cseh@gmail.com*

Article History
Volume 6, Issue 12, 2024
Received: June 10, 2024
Accepted: July 5, 2024
doi:
10.48047/AFJBS.6.12.2024.4957-4968

Abstract-Introducing the Kriper blockchain, a revolutionary countermeasure to the growing risks that Internet of Things (IoT) applications encounter. Kriper complies with the strict data integrity and security criteria of the commercial world by emphasizing important elements like strong message services and distributed storage in this proposal. Kriper's network really shines as a defense against any data breaches, especially in light of the recent spike in attacks against IoT applications. This paper emphasizes how well the network protects a range of IoT applications that are susceptible, such as wearables, smart homes, smart grids, and healthcare systems. Kriper compensates for the storage-related deficiencies in filtering power, hence providing a strong defense against cyberattacks. Now-a-Days The number of attacks against Internet of Things (IoT) applications is steadily rising. This study explains how various IoT applications, including smart grids, smart homes, wearables, and healthcare applications, are vulnerable against assaults because of insufficient filtering power caused by storage problems. This results in data breaches and lower data confidentiality and integrity. This article introduces the Kriper blockchain, which focuses on providing the corporate world with the data integrity and security requirements with purported features such distributed storage and message services.

Keywords: Block Chain, IoT, Kriper, Security, DAG Chain.

1. Introduction

Cyberattacks have increased recently, and the IoT has witnessed an increase in applications imposing sensors and smart devices. They encounter security issues, particularly given how many devices are compact and open to DDoS, ransomware, bruteforce, and other attacks.

Secure communication and lightweight encryption are more crucial for ensuring safety than secrecy, integrity, and availability.Companies are also investigating it for real-time data transfer and safe data management.

IoT applications contain layers that are categorized into three categories: the physical layer, the network layer, and the application layer. Each category has vulnerabilities based on the functioning of the layer [11].

Some businesses use blockchain for data integration or audits, but they don't completely understand it. due to that Kriper, a blockchain created specifically for business needs, enters the picture. Additionally, it is a decentralized network, allowing data to be divided into several nodes that are connected to one another and offers security, flexibility, and storage capacity for both large files and messages with few bytes. The following IoT devices have been impacted or attacked by attackers:

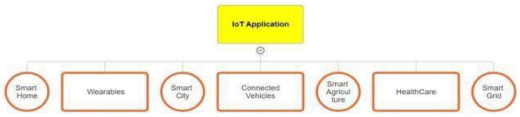

Figure 1. Lightweight Encryption

1.1. Issues and Security Challenges in IoT

Many traditional applications have become smarter thanks to IoT technology, yet there are still significant security and privacy concerns. These difficulties are depicted in several layers of IoT applications. IoT devices have limits, and numerous assaults can be launched at different layers.

The most difficult challenge is how to integrate IoT usage regarding data protection and security. For example, consider the health care sector, which employed IoT apps to remotely monitor users, which resulted in data breaches [3].

Basic approaches are ineffective since IoT devices can only perform a limited set of functions; instead, they use cryptographic algorithms with fewer keys and more straightforward processing. The system needs to take care of the security issues present in each tier.

a) *Node capture attacks*: As the name implies, this type of attack is a little challenging to identify because the attacker can capture the devices. Thus, the attacker can obtain practically all pertinent information about the target device and record these kinds of attacks.
b) *Eavesdropping*: This assault may take place if two IoT smart devices are not capable of sending data to each other quickly enough.
c) False data The IoT-based devices are restricted to a specific capability due to the deployment of sensors in multiple locations to communicate between layers, which makes it easier for attackers to introduce inaccurate or fraudulent information into the devices.
d) *Spoofing*: In the network layer, because smart devices have limited resource functionality, an attacker may get access to the network and be able to send fake or inaccurate data to other nodes or devices in the area.

e) *Denial-of-service (DoS) attacks*: This type of cyberattack involves the hacker or assailant slowing down the entire Internet of Things device so that data cannot be transferred to other smart devices via sensors and more [7].
f) *Unauthorized access*: The attacker may employ a variety of techniques to steal legitimate user credentials, take control of the device, and provide false information to the linked smart IoT devices.
g) *Phishing attempts*: Since smart devices can send information to other smart devices by using their identities, an attacker might try to send their own information.
h) *Malicious assaults*: When using IoT apps, devices are vulnerable to attacks because of unreliable wireless communication, which allows an attacker to inject malicious code into the target device.
i) *Policy enforcement*: Policy, which permits users to utilize smart devices, is one of the primary security issues in IoT applications. To protect user privacy, sufficient police must be created in accordance with the application's specifications [5][15].

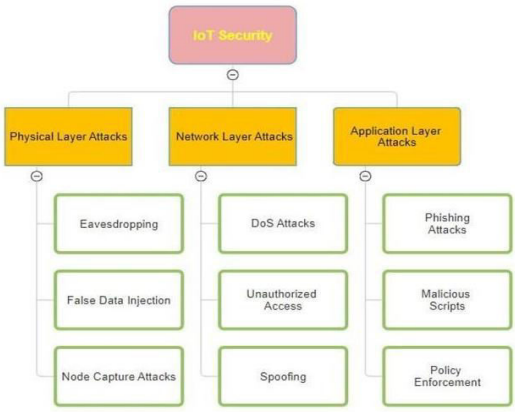

Figure 2. IOT Security

1.2. Privacy in IoT

The physical, network, and application layers are the three main tiers of the Internet of Things (IoT). Numerous smart gadgets are deployed at the physical layer to collect copious amounts of data about their surroundings.

The three main processes in this data collection process are collection, consolidation, and analytics. In order to extract useful information, sensors and smart devices first collect raw data, which is then aggregated and processed [2].

However, privacy issues become a major problem during the data collecting and processing. For instance, illegal access to patient information might result in privacy violations in IoT-enabled healthcare systems.

Similar privacy concerns can arise in smart cities when user location and travel data is collected or leaked. To this privacy preservation techniques need to be addressed [8].

2. Related Work in Block Chain

A decentralized network called a blockchain is used to store transactions or data. In the case of Ethereum [18], it is possible to store and/or validate a specific logic on the blockchain using Smart Contracts because a blockchain like Bitcoin or Ethereum only maintains a limited quantity of data [4].

Files cannot be supported in the blocks of Ethereum, Bitcoin, and other cryptocurrencies since they are linear (approving blocks one after the other). If they did, the size of the blockchain would be known, which would limit the number of miners to those who have adequate RAM and storage capacity to create fresh blocks of data. Thus, working with large amounts of data would unnecessarily slow down mining and the approval of new blocks until it could no longer be sustained [1].

File coin a blockchain is similar to the in that it handles vast amounts of data, but it lacks permissions and laws. Certain blockchains, such as Ethereum and Bitcoin, are linear in nature (verifying blocks one after the other) and do not allow the transfer of big data files to neighboring smart devices. And now for more blockchains: Data Coin, File Coin, Proof of Storage (PoSt) is a revolutionary approach that complements PoW and PoS by rewarding users for lending their excess storage space to the network. These blockchains [9], like Data Coin and File Coin, are also linear in nature, but they store their data in files, P2P, and miners. Similar to the Kriper blockchain, file coin allows file storage and P2P transfer.

Table 1. Comparative Analysis of Blockchain Features

Blockchain	**Data Storage Capability**	**File Support**	**Consensus Mechanism**	**Noteworthy Features**
Bitcoin	Limited	No	Proof of Work	Pioneering cryptocurrency [14].
Ethereum	Limited	No	Proof of Stake	Smart Contracts [12].
File coin	Extensive	Yes	Proof of Storage	Decentralized storage network
Kriper Blockchain	Signific ant	Yes	Leighton-Micali Signature	Two-layer paradigm, enhanced privacy [16]
DAGChain Technology	Abundant	Yes	Proof of Storage	Efficient file storage within blockchain [20].

2.1. Literature Review

Table 2. Cryptocurrencies and Blockchain Protocols

Title	**Author**	**Year**	**Related Work**
"Bitcoin: A Peerto-Peer Electronic Cash System"	Nakamoto, S.	2008	Double-spending preventionwithout intermediaries [17].
"Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform"	Buterin, V.	2013	Next-gen platform for smartcontracts and applications
"Filecoin: A Decentralized Storage Network"	Filecoin Project	2017	Decentralized revolution in internet services [13]
"BlockchainBased Cryptography for Enhanced Security and Privacy"	Leight on, T., & Micali, S.	2018	Integration for decentralized immutable security.
"Future Generation Computer Systems"	María Isabel Rojo Rivas	2022	Exploration of future generationcomputer systems advancements.

2.2. Differences between Kriper Blockchain and Alternative Existing Blockchains

Table 3.Blockchain and Alternative Existing Blockchains

Aspect	Traditional Blockchain	Kriper Blockchain
Storage	Linear, limited capacity	Two-layer model, scalable, diverse data storage [10].
Mining	PoW/PoS, high complexity	PoW, low complexity
Speed	Slower growth, high competition	Faster growth, low competition
Privacy	Traceable wallet addresses	Hash-based user identification for increased privacy
Data Flexibility	Limited, specific data types	Allows any type of data storage
Compartmentalization	Limited options	Private compartments, data segregation
Network Structure	Singlelayer, miner competition	Two-layer, interconnected work pools
Viability	Scalability limitations	Successfully tested in various environments
Use Cases	Limited, currency transactions	Diverse business applications: micro messages, IoT, file storage

3. Proposed Methodology

3.1. Overview of Kriper Blockchain Design

a) *Two-Layer Paradigm:*Kriper Blockchain uses a two-layer architecture to improve performance. In order to identify users of this structure, a hash value that is part of the structure is used, together with the Leighton-Micali signature.

b) *Leighton-Micali Signature:* The Leighton-Micali signature allows for user authentication on the Kriper Blockchain [6]. This cryptographic technique makes sure that user interactions are secret and secure, making it difficult to track the movements of users.

c) *Block Validation:* Miners validate new blocks by comparing them to the two blocks that came before them in order to ensure the validity and integrity of the proposed block. The thorough validation guarantees the blockchain's resilience.

d) *DAG Chain Technology:*Kriper stores files in the blockchain effectively by utilizing DAGChain technology. The data is arranged in a secure and easily accessible way thanks to this Directed Acyclic Graph (DAG), which makes file storage and retrieval easy [20].

e) *Disk-Rich Workstations:* The Kriper network is made up of multiple computers with large amounts of disk capacity. These workstations with lots of disk space are essential for holding important files pertaining to the DAG Chain technology of the blockchain, enabling security upkeep, data backups, and validity checks.

f) *Algorithm selection- Leighton-Micali (LMS):* The Leighton-Micali signature (LMS) was selected for user identity verification due to its lightweight design. Particularly chosen for its effectiveness in processing user identity even with constrained computer resources is this method, which has lower key lengths.
g) *Privacy Preservation:*Kriper Blockchain places a high priority on maintaining user privacy by using safe algorithms and encryption methods. With blockchain applications, where user data and interactions require strong protection, privacy becomes especially important.
h) *Efficient Data Transmission:* The utilization of the LMS technique guarantees quick processing of user identity within the Kriper network, even in the event of resource constraints. Maintaining this efficiency is essential to the overall performance and responsiveness of the blockchain.
i) *Integration of DAG Chain:*Kriper's architecture incorporates DAG Chain to enable accurate and safe data storage on the blockchain. This method provides a special way to handle big files and data sets without sacrificing the effectiveness of the network.

Even with the ECSA private key method, which is frequently employed in blockchains because of its inconsistent computational results. Because the LMS method is lighter due to the shorter key lengths, it was chosen after extensive research on a variety of algorithms, which demonstrated that it is faster than the majority of algorithms. The LMS is selected because it employs the DAG Chain, which keeps files or data in the blockchain. Other algorithms are available for lighter keys and data transmission modes, but the DAG Chain demands the most precise analysis.

3.2. Proof of Work in Blockchain

Kriper differs from systems like Bitcoin in that it uses a Directed Acyclic Graph (DAG) structure to store data instead of a linear blockchain. This DAG allows for many connections for validation by connecting blocks in a way that resembles a web.

The miner must validate two earlier blocks and link their data to the new block to add a new block to the Kriper DAG. The integrity of the data is guaranteed, and security is improved.

Unlike linear blockchains, this approach allows blocks to link to a variety of different blocks. By allowing other nodes to check and confirm the same information, this novel approach offers robustness and reliability. Every new block must be linked to at least two older blocks, which helps to keep the network's dependability and integrity.

Adding the number of links between the nodes greater communication and data security. A linear blockchain model requires approval from every member of the network before the most recent block is added, and it requires the entire blockchain to synchronize with everyone before moving on to the following block. This causes a delay in the process that doesn't end until everyone is prepared, which inhibits the chain's expansion.

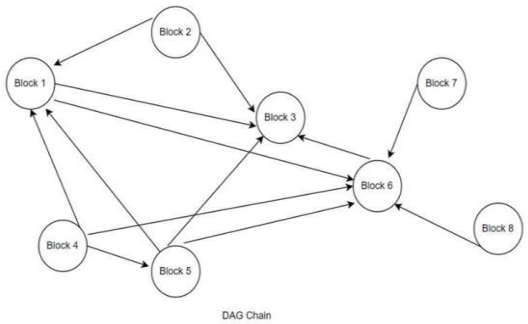

Figure 3. Work in Blockchain

This contrasts with situations where a quick method to add blocks is required, such as with IoT communications, logs, traces, or many transactions. In these conditions, waiting for

everyone to catch up is not feasible, needing a more dynamic approach to ensure rapid progress. And this is the main goal to choose DAG Chain model in this Kriper Blockchain DAG Chain. The Directed Acyclic Graph (DAG) in Kriper Blockchain doesn't expand uniformly, potentially creating imbalances in its growth between different data segments. Hence, with every new block, two key procedures occur: an asynchronous synchronization with the network and optimization steps are implemented to maintain a balanced structure and ensure consistent performance.

The asynchronous update guarantees that all network participants maintain a synchronized view of the DAG Chain, preventing duplication of blocks or transactions. In parallel, the optimization process encourages miners to seek out validated blocks with fewer connections to subsequent blocks or orphaned validated blocks with no references to later blocks, ensuring their inclusion in new blocks and preventing them from being forgotten over time. Miners must validate transactions and execute a Proof of Work (PoW) to create a new block.

Identical to Bitcoin's Hash cash method, Kriper's Proof of Work (PoW) mechanism intentionally keeps the difficulty level low to deter network manipulations. This ensures the network safer against spam and Sybil attacks while successfully limiting the rate at which blocks accumulate inside the DAG Chain [20].

A miner using hash cash must solve a challenge via exhaustive trial and error (attempting every potential outcome in a short period of space). For one to solve this puzzle, you must find a number (nonce) that, when determined by brute force, causes a hash to start with a particular number of zeros, as indicated by the network difficulty at that moment.

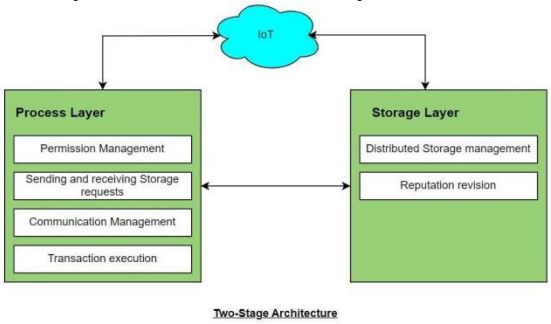

Figure 4. Two Stage Architecture

3.3. DAG Chain

As previously noted, the Kriper blockchain is known as DAG Chain. It is comprised of a Directed Acyclic Graph (DAG) in which data blocks, referred to as validated nodes, are connected to one another in the form of a graph.

Packets were available in three distinct states:-

1. Recorded and Validated
2. Validated(V)
3. On Hold

There are mainly 5 points need to be noted:-

1. In DAG Chain, blocks—also known as validated nodes—are proposed and shared among all network pools.
2. Validators verify the correctness of the content and its connections to earlier DAG blocks. Note that the equation is centered using a center tab stop.
3. Each miner independently confirms and verifies the suggested blocks and the transactions they contain.
4. Pool librarians store the validated blocks after they have been verified.
5. These blocks are recorded and added to the DAG.

Chain, which is a verified and connected transaction graph.

The entire validation process is hosted by the Process Layer, which is mostly controlled by miners to prevent orphaned or inadequately certified nodes. Comprehensive maintenance and validation duties are used to ensure the integrity and security of the DAG Chain.

4. Proposed Architecture

4.1. The Kriper network

Kriper's network is what makes it strong which separates the network into two layers.
Requests are received through the process layer, and only the execution layer above can access the storage layer, which stores data. The DAG Chain is processed by the execution layer.
Execution Layer: This layer is responsible for recording transactions onto blocks, which form the DAGChain. Two different kinds of machines are used in linked work pools in this process [16]:

a) *Miners*: The processing capacity that miners possess allows them to validate transactions and add new blocks to the DAGChain.
b) *Librarians*: Participate in the Process Layer, have storage space, and oversee securing the DAGChain.

Network resilience is improved via interconnected work pools, which increase the number of machines available and effectively handle large numbers of requests. Adding further mining chances, the introduction of new blocks is contingent upon two prior outcomes. These networked pools consist of two involved parties:

a) *Miners*: Verify transactions and contribute fresh blocks to the DAGChain.
b) *Librarians*: Protect the Process Layer's DAGChain.

To prevent manipulation by owner-controlled pools, newly hired librarians are assigned to either the storage or execution layer based on machine attributes and a random component.
Miners are supported by librarians at the Execution Layer, who make sure that new node blocks are properly incorporated into the DAGChain [16]. They are essential in helping librarians in the Storage Layer and Process Layer pools replicate the DAGChain. The steps for allocating mining pools are as follows:

a) *The Kademlia Protocol*: uses peer-to-peer connections to identify members who have the lowest latency Librarians: Protect the Process Layer's DAGChain.
b) *Owner Choice*: Considering disk space and network speed, system owners decide whether to become miners or librarians based on client demands.
c) *Pool Addition*: Miners and libraries sign up for pools according to future requirements and available space.
d) *Conflict Avoidance*: To avoid conflicts of interest, pools are made up of nodes from different IP addresses or networks.
e) *Frequent Re-evaluation*: Every two years, appropriate groups are reevaluated.

The pool size determines the network size, with the formula $2z + 1 = y$, adapting as the network grows. The Process Layer in the Kriper network manages crucial tasks:

a) *Transaction processing*: manages and keeps track of transactions, replicating them in the Storage Layer and storing them in the safe DAGChain.
b) *Huge File Storage*: Requests for huge files to be persistent are handled by the execution layer.
c) *DAGChain Optimization*: Performs actions to keep the blockchain's integrity intact.
d) *Permission management*: Uses tools like user balance and network access settings to control user content access.
e) *Communication Oversight*: Uses the Kademlia protocol to regulate node communication for file exchange and DAGChain replication.

The Storage Layer: The storage layer is managed by the librarians; DAG chain cannot handle the files in this layer. The files are divided into multiple parts or pieces, which are then stored

in the layer. Additionally, the chunks of file pieces are distributed in various libraries through the use of a protocol known as kademila.

Since the layer splits the files into manageable chunks or pieces and distributes them throughout the storage layer, the data in that piece will be shared with other librarians even if a single portion disappears or becomes missing amongst connected nodes. This will become apparent when content from lost nodes and dispersed storage is equally disseminated to other librarians. The creator of the files stored in the layer will validate the packets, or if a packet is identified by KRP, KRP will reach out to that packet.

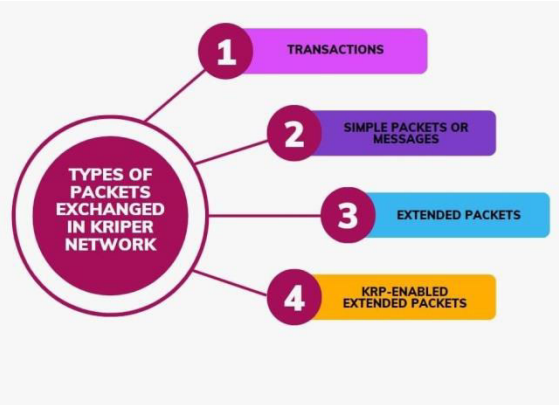

Figure 5. Types of Packets Exchanged in the Kriper Network

The regular packets used to conduct KRP transactions between the accounts are called transactions. Furthermore, using straightforward packets for IoT device sensors to carry out quick connection for dependable transfer; the majority of these packets are free and designed for quicker processing and storing and larger files or documents are utilized with extended packets. Extended packets are also used in KRP to conduct KRP transactions. KRP charges for these kinds of packets, and users must pay a price each time they access a document containing an extended packet.

Purchasing KRPs for other members despite value fluctuations Although the value of KRP can fluctuate and it can be exchanged for other cryptocurrencies or fiat currency, you can purchase or sell tokens by getting in touch with different sellers. A vital role that miners and librarians play is ensuring the network functions properly. In addition to creating new tokens through mining, they also receive KRP for storing data on the network.

All nodes in the mining pool share the rewards (KRP) that miners at the Process Layer in the bitcoin network receive for producing new blocks through mining. Rather than mining on the Storage Layer, librarians store data on the network. They are rewarded based on a reputation system that takes into account things like the quantity of space offered, the length of time spent collaborating, the KRP holdings, and the information that has been stored. More reputable librarians are awarded a more equal share of KRP, which promotes ongoing cooperation in providing storage space to the network. Thus, whereas rewards at the Process Layer are derived from mining, awards at the Storage Layer are determined by a reputation system that is connected to different contributions and pledges made to the health of the network.

Thirty percent of the highly regarded librarians in this network are under constant observation. For example, among the top 10% of credible librarians, there is one with three days of collaboration, one terabyte of storage, and twenty percent of busy information. But if the librarian experiences network outages, doesn't receive any new files, or loses stored KRPs during a transfer, their reputation may suffer. Reputable librarians receive regular rewards from the network in three different ways: they can store a lot of data for KRP rewards, rank in the top 30%, or participate in the Process Layer and earn 0.5 KRP for each block that is successfully mined and verified. Every eight hours, reputation is adjusted, awarding 0.5 KRP

to all librarians in the top 30% for their consistent network contributions. This guarantees a consistent reward for their hard work.

With cryptocurrencies and the concerns about the 51% attack, particularly in smaller communities where manipulation is easier. Unlike other blockchains, Kriper's design prevents coordinated attacks because the blockchain randomly assigns miners to pools. The DAG-based architecture and this unpredictability make it unlikely that attackers will cooperate across pools or even be in the same pool. In traditional linear blockchains, every member pool mines the same next block. Nevertheless, in a DAG-shaped blockchain such as Kriper, where blocks are connected by various connections, coordination becomes exceedingly challenging, providing additional protection against the 51% assault.

To incorporate file splitting into Kriper, a modified Google File System (GFS) model was first investigated. Kriper uses a P2P protocol instead of GFS, which prevents the disk space waste that comes with equal block sizes. Users individually prepare and split files according to the guidelines: every size file is broken into at least five parts, which are then replicated on five different PCs. With adjustable split sizes and an unlimited number of parts per file, the maximum file size for fast transfers is 50 MB.

The data flow follows a user-initiated 'Request Transaction':

a) Users ask the nearest miner to download files for them.
b) To confirm user context, file existence, SHA hashes for chunks, Key Resource Points, and access privileges, the miner gets in touch with a librarian in their pool.
c) The miner provides the client with access to the original file transaction block after successful checks, and the client notifies librarians of its address.
d) Librarians validate the transaction by looking the necessary files in the DHT using a real-time copy of DAGChain. The file transfer is started by the closest librarian.
e) BitTorrent is used by the closest librarian to provide decentralized, parallelized file fraction transmission across several nodes, which guarantees speedy downloads. This method maximizes the efficiency of file transfers within the decentralized Kriper network.

5. Result and Discussion

Kriper's implementation of the suggested data flow demonstrates how effective it is for decentralized file transfer. The comparison with Google File System (GFS) makes clear that this technique overcomes the shortcomings of existing models and prioritizes peer-topeer (P2P) communication for optimal data distribution.

Reduced disk space waste, adaptable file splitting, and the use of BitTorrent for decentralized and parallelized file transmission are the main benefits. Efficient handling of different file sizes is ensured by the 50 MB restriction for rapid transfers. Together with DAGChain verification, user interaction with miners and librarians creates a trustworthy and safe transaction procedure.

5.1. Comparison with Previous Research

a) *Google File System (GFS):* By eliminating identical block sizes and using a P2P protocol, the Kriper model gets around GFS's constraints and shows better disk space utilization and file splitting flexibility.
b) *BitTorrent Protocol in File Transfer:* Our method is based on earlier studies that made use of the BitTorrent protocol to facilitate effective file transfers. Kriper shows how flexible and powerful this idea is by extending it to decentralized networks.

5.2. Advantages of Using DAG Chain Model in IoT Devices

a. *Distributed Storage:*Kriper Blockchain supports permissioned distributed storage, which means it can be used to store data decentralized while simultaneously ensuring that only authorized parties have access to the data. Kriper Blockchain is community-based, which means that anyone who wishes to engage in the network can do so.

b. *Micro Message Services*: Kriper Blockchain offers micro message lightweight services, which means it can be used to swiftly and efficiently send and receive small amounts of data.
c. With the above-mentioned features of Kriper can be more helpful to secure the IoT devices in terms of security and integrity of data.

6. Conclusion

In conclusion, the Internet of Things (IoT) introduces challenges such as security vulnerabilities and scalability issues. Kriper blockchain emerges as a promising solution by addressing these concerns through its double-layer approach, prioritizing speed without compromising security. Unlike traditional blockchains, Kriper utilizes data obfuscation and distinct permissioned network segments to safeguard against unauthorized access in resource-intensive ways. Its adaptable design tackles issues like information propagation control and participant compensation in the storage layer, making it a more efficient and adaptable solution for real-world IoT applications. By prioritizing data protection and permissions enforcement, Kriper stands out as a secure and high-performance blockchain, offering a compelling alternative to address the disadvantages associated with IoT implementations on traditional blockchain platforms.

References

[1] P. Tasatanattakool, C. Techapanupreeda, Blockchain: Challenges and applications, in: 2018 International Conference on Information Networking, ICOIN, 2018, pp. 473–475, http://dx.doi.org/10.1109/ICOIN.2018.8343163.
[2] G. Lize, W. Jingpei, and S. Bin, “Trust management mechanism for Internet of Things,” China Commun., vol. 11, no. 2, pp. 148–156, 2014.
[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: Application areas, security threats, and solution architectures,” IEEE Access, vol. 7, pp. 82721–82743, 2019.
[4] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, “Trustchain: Establishing trust in the IoT-based applications ecosystem using Blockchain,” IEEE Cloud Comput., vol. 5, no. 4, pp. 12–23, Jul./Aug. 2018.
[5] M. A. Khan and K. Salah, “IoT security: Review, blockchain solutions, and open challenges,” Future Gener. Comput. Syst., vol. 82, pp. 395–411, May 2018.
[6] Y. Song, X. Hu, W. Wang, J. Tian, Z. Wang, High-speed and scalable FPGA implementation of the key generation for the Leighton-Micali signature protocol, in 2021 IEEE International Symposium on Circuits and Systems, ISCAS, 2021, pp. 1–5, http://dx.doi.org/10.1109/ISCAS51556.2021.9401177.
[7] I.-C. Lin and T.-C. Liao, “A survey of blockchain security issues and challenges,” Int. J. Newt. Security, vol. 19, no. 5, pp. 653–659, 2017.
[8] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating critical security issues of the IoT world: Present and future challenges,” IEEE Internet Things J., vol. 5, no. 4, pp. 2483–2495, Aug. 2018.
[9] L. Zhou, L. Wang, Y. Sun, and P. Lv, “Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation,” IEEE Access, vol. 6, pp. 43472–43488, 2018.
[10] O. Novo, “Blockchain meets IoT: An architecture for scalable access management in IoT,” IEEE Internet Things J., vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
[11] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 881-888, Jan. 15, 2021. DOI:10.1109/JIOT.2020.3008906

[12] G. Wood, Ethereum: A secure decentralized generalized transaction ledgerEIP-150 REVISION.
[13] V. Vatsalya, S. Arora, A. Jain, T. Patil, S. Patil, Marine hull insurance using a private blockchain, file coin protocol and smart contracts, Int. J. Adv. Res. Compute.Sci., 9 (3)(2018)URL: (http://ijarcs.info/index.php/Ijarcs/article/view/5759).
[14] S.N. Sunny King, PPCoin: Peer-to-peer cryptocurrency with proof-of-stake, 2012, URL: (http://www.peercoin.net/).
[15] T.A. Ahanger, A. Aljumah, Internet of things: A comprehensive study of security issues and defense mechanisms, IEEE Access 7 (2019) 11020–11028, http://dx.doi.org/10.1109/ACCESS.2018.2876939.
[16] María Isabel Rojo-Rivas, Daniel Díaz-Sánchez, Florina Almenarez, Andrés Marín-Lopez, "Kriper: A blockchain network with permissioned storage",Source: Future Generation Computer Systems, 2022, Elsevier B.V. DOI:https://doi.org/10.1016/j.future.2022.08.006,
[17] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, URL (https://bitcoin.org/bitcoin.pdf).
[18] F. Leal, Performance Evaluation of Private Ethereum Networks, 2020, http://dx.doi.org/10.1007/s42979-020-00289-7.
[19] Ahmed Afif Monrat,Olov Schelén, (Member, IEEE), AND KARL ANDERSSON, (Senior Member, IEEE), A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities Volume 7, 2019. (http://creativecommons.org/licenses/by/4.0/)
[20] Li, L., Huang, D., & Zhang, C. (2023). An Efficient DAG Blockchain Architecture for IoT. IEEE Internet of Things Journal, 10(2), 1286-1287.https://doi.org/10.1109/JIOT.2022.3206337.