LAUTECH Journal of Engineering and Technology 19 (3) 2025: 133-141
10.36108/laujet/5202.91.0321

Blockchain Security Model for Minimising Free-Riding in a Peer-to-Peer Network

[1]Ogundoyin I. K., [2]Ojo O. E., [2]Ayilara-Adewale O. A., [3]Olatunde Y. O., and [4]Akwagha L. E.

[1]Department of Computer Science, Osun State University, Osogbo, Nigeria.
[2]Department of Information Technology, Osun State University, Osogbo, Nigeria.
[3]Department of Cyber Security, Osun State University, Osogbo, Nigeria.
[4]Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria.

Article Info

Article history:

Received: April 30, 2025
Revised: June 21, 2025
Accepted: July 17, 2025

Keywords:

Peer-To-Peer Networks,
Blockchain,
Network Security,
Free-Riding,
File Sharing.

Corresponding Author:
ibraheem.ogundoyin@uniosun.edu.ng
+234(0)8032481441

ABSTRACT

Peer-to-Peer (P2P) networks are unique innovations utilised in file sharing applications to accomplish better execution and evade a weak link. They can be centralised and decentralised, structured and unstructured. The prevalence of the P2P network has drawn in various attacks, including Free Riding, which decreases the adequacy of the network. Although numerous moderation strategies have been proposed to diminish the effect of such attacks, minimising free-riding is still a major challenge on the Internet. A P2P-based mechanism called blockchain technology is a promising tool capable of addressing this challenge due to its distinct features, such as transparency, provision of a highly secure platform, immunity to attackers, and cost-effectiveness. This research proposes a blockchain-based security structure for P2P networks to address free-riding and is modelled using an incentive approach. The proposed framework uses blockchain hash value to connect each peer with the associated super peer that grants an upload or a download, validating the peer and forming an immutable block in the network. The system was tested within a peer-to-peer file-sharing system simulation scenario and implemented using Java programming language. The simulation results show improved performance in identifying and countering free riders in the network with a fairness index of 0.8 to 0.9, blocking approximately 400 peers, and creating more than 4500 validated blocks at 2500 peers.

INTRODUCTION

On the Internet, numerous applications use document sharing through Peer-to-Peer (P2P) frameworks. For two decades now, P2P frameworks have arisen as a critical social and specialised infrastructure. P2P frameworks give a foundation to networks that share CPU cycles and storage space (for instance, FreeNet, Gnutella), or that help relational collective conditions. The two main components that encouraged the new hazardous development of these frameworks were the minimal expense and high accessibility of huge computing and storage resources, and the expanded network connectivity (Ripeanu, 2001).

P2P network has emerged as a famous method to share information across a large peer population, offering a few benefits over the centralised approaches. P2P networks connect each node with other nodes in the network, without including other physical connections. Each node in a P2P network acts as both server and client, so the bottleneck of client-server architecture is eliminated (Jafari *et al*., 2015). That is, the node can convey solicitations to different nodes in the network and similarly gets and reacts to their requests. The node or peer assumes the roles of a client and a server simultaneously. It changes from the customary client-server model where a client can just send solicitations to a server

and wait for the server's response (Padhy *et al*., 2012). In a conventional client-server network, communication exchange utilises central servers. These servers can store data and handle demands over the network. They give platforms on the network where clients can get answers to their particular queries. Servers additionally take on the regularly centralised model by providing asynchronous communication between clients (Musa *et al*., 2019). As of late, P2P networks have grown dramatically in prevalence and usage. P2P document sharing has become quite possibly the most famous internet activities. According to investigative results, around 50–65% of "downstream traffic" and 75–90% of "upstream traffic" on the Internet are the consequences of P2P record-sharing applications (Liu and Antonopoulos, 2010). The advantages of P2P file sharing are good scalability and high bandwidth in comparison with the client-server technology for file distribution (Masinde and Graffi, 2020).

Despite the need for P2P frameworks and their widespread execution, their performance is influenced by an issue: the phenomenon of free-riding. Free-riders are non-collaborative clients who do not contribute any resources to the network while consuming resources contributed by different clients (Edirimannage *et al.,* 2025). The presence of free-riders influences the health of the service as it causes trouble for other nodes, like delays, and the wasting of resources. This influences the capacity of P2P frameworks to meet their general purpose, which is sharing and collaboration (Alotibi *et al*., 2019). Research has shown that the spread of free-riding companions can be damaging. It may likewise decrease the worth of file sharing in the network and further transform it into a sick network. Unfortunately, the P2P framework doesn't have a central regulator equipped for observing client performance. Hence, the detection and prevention of malicious behaviours in this environment have become a major challenge. The ideal approach to managing nodes and urging them to participate is a crucial issue (Shareh *et al.,* 2019).

Blockchain innovation gives a promising mechanism for managing peers in a P2P system because of its qualities, like transparency, decentralisation, and anti-tampering (Li *et al*., 2019).

Blockchain is a peer-to-peer network-based technology, where the client can transact straightforwardly without the assistance of any trusted authority. This innovation is utilised in developing applications such as voting systems, messengers, social networks, prediction markets, smart contracts, and substantially more (Vimal and Srivatsa, 2020). A blockchain is regularly referred to as a collection of distributed databases that comprises every public transaction, record, and digital event, such that data is shared between the participating peers. Each transaction is confirmed, and it can't be eliminated. Blockchains are made of blocks of transactions that are chained together through a cryptographic hash of the previous block (Vivekanadam, 2020). The research attempts to foster a viable system for forestalling free-riding in a peer-to-peer network using blockchain technology.

The foremost research with an incentive mechanism to avoid free-riding in the P2P network was conducted in 2003. Several utility capacities were proposed to assess the commitment of each peer, but the system did not consider the dangerous swindling issue and the utility capacity as basic (Ramaswamy *et al.,* 2003). A multi-level framework dependent on computational riddles to protect against Sybil attacks was designed. This framework recommended making a tree with roots as a trusted and reliable node. The root can permit other

confided-in hub nodes to join the system, Internet Service Providers. Subsequently, acquiring different personalities becomes hard for the attackers (Rowaihy *et al*., 2005).

Researchers have investigated methods to mitigate free-riding in peer-to-peer (P2P) networks, where peers consume resources without contributing. The primary countermeasures fall into three categories: game-theoretic approaches to enforce cooperative behaviour, economic incentive mechanisms to promote resource sharing, and social network-based strategies to enhance trust and collaboration among peers (Yijiao and Hai, 2008). For instance, a game theory-based mechanism that uses incentives and service differentiation was designed (Ma *et al.,* 2006). Moreover, another peer-assisted streaming model using game theory for limiting free-riding was proposed by Ojo *et al.(*2020). Biaou *et al.* (2020) applied the game hypothesis model utilising the stochastic model to alleviate free riders in a partially centralised peer-to-peer network.

Some researchers investigated the utilisation of a mitigation approach specific to the Freenet P2P network. The scheme proposed a route forecast model to discover the path of the message and recognise it if it redirects the path (Tian *et al.,* 2014; Raza *et al.,* 2024). Furthermore, Alotibi *et al.* (2019) proposed a points system approach as a model of defeating free-riding conduct in peer-to-peer networks and contrasting its viability and the original BitTorrent protocol.

In addition, several kinds of research have been conducted using the features of blockchain technology to achieve viable solutions. To mention a few, a conceptual model was designed for managing the Protected Health Information (PHI) data, which is derived from several healthcare providers by relying on blockchain technology in the peer-to-peer overlay network (Rahmadika and Rhee, 2018). A model that leverages blockchain technology to achieve decentralised parked vehicle-assisted fog computing was proposed by Huang *et al. (*2020). A blockchain-based, decentralised and truthful framework for mobile device cloud was developed in (Wang *et al.*, 2020). The system enables decentralisation and prevents dishonesty by incorporating a plasma-based blockchain into the mobile device cloud. Further, a data management method for the digital twin of products based on blockchain technology is proposed by Putz *et al. (*2021). Cryptocurrency incentivised crowdsourced P2P Content Delivery Network named CROWD-CDN was developed. The CROWD-CDN employed blockchain-based cryptocurrencies and smart contracts for the monetisation of peers (Yousafzai *et al.,* 2021). This work is motivated by the robust solutions achieved by existing blockchain solutions; hence, an effective blockchain-based model to alleviate free-riders in the P2P network to the barest minimum was proposed.

Kurdi *et al.* (2020) developed the Adjusted Free Market-Inspired Approach (AFMIA), an adjusted free market-inspired model which considers resources as goods that have dynamic costs that depend on the measure of supply and demand, and the peers have abundance, which can increase by giving resources and be spent on consuming the resources provided. This work is motivated by the robust solutions achieved by existing blockchain solutions; hence, an effective blockchain-based model to alleviate free-riders in the P2P network to the barest minimum was proposed.

METHODOLOGY

The proposed blockchain security framework, as shown in Figure 1, consists of a peer module, a blockchain module, and a record module. Resources within the system are exchanged among peers using a mesh-based overlay topology to avoid peer starvation and a continuous flow of data in the

network. The peer module effectively manages file exchange between request peers and sender peers. It ensures the requesting peers can download resources within a time frame. Another function of the peer module is tracking the activities of each participating peer, which is embedded in the Timer. After the first download, each peer is qualified for a free solicitation time from the hour of download, during which they should add to the network by transferring resources; otherwise, subsequent requests are denied. The initial download demands from peers are approved by default, and the timer is initiated. For the following download demands, the peer module monitoring tool sends a notification to neighbouring peers within the mesh topology. If the peer has contributed at least *x* valid data files, the timer is analysed against the assigned time for testing. Assuming the hour of the solicitation is inside the time for testing, the download demand is supported. Assuming the time for testing has lapsed, the number of transfers by that client is checked. Assuming the peer transferred at least x + n, (where **"x"** is minimum required threshold of data."n" **is** adaptive or incremental value that accounts for dynamic conditions such as network load, peer behavior, or contribution history) the download demand is supported and the clock is restarted, else, the solicitation is denied, and resulting download demands are additionally denied if the peer neglects to contribute any information.

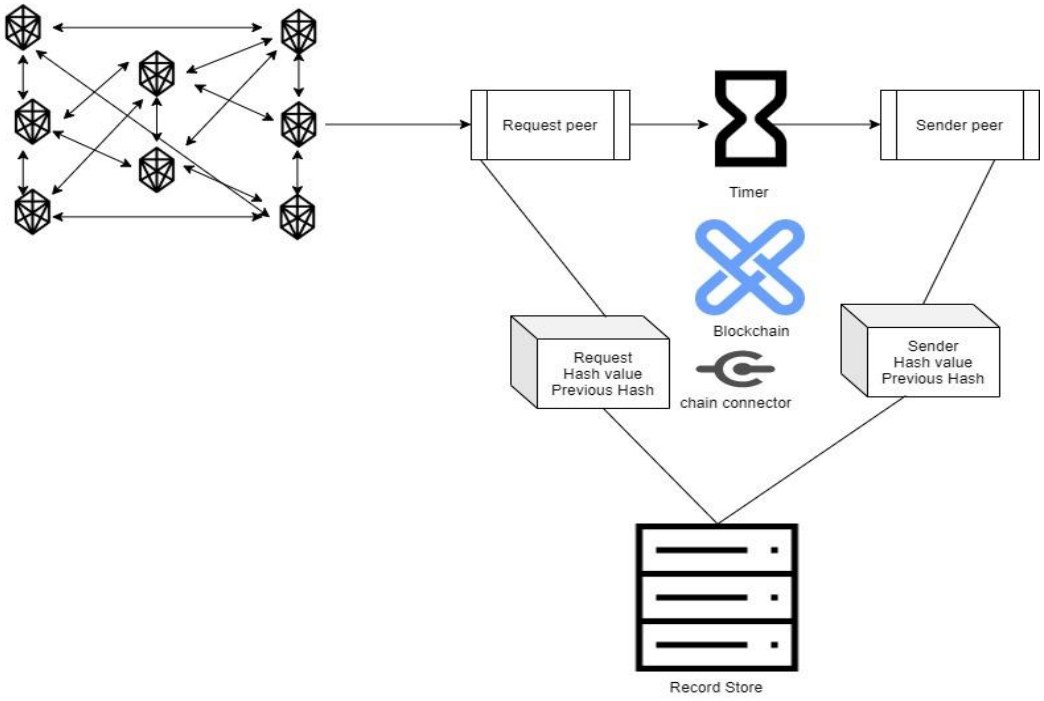


Figure 1: Conceptual Model of the Blockchain Security System.

The blockchain module consists of three elements, which are:

i. The data of all transactions within the timeframe or stamp
ii. The hash value, which can be described as a unique identifier, and
iii. The previous hash value.

The blockchain is also reviewed in that each block is validated by miners, and an invalidated block cannot form the chain. The record stored is permanent and immutable; new records can be added to an existing block, but the previous record cannot be changed. Changes or transaction history are visible to the public, so the peers can easily identify and trace the history of any peer.

The following validation checks are performed on information received from requested peers:

i. The message is first unscrambled by utilising the private key.

ii. The authenticity of peers is confirmed to ascertain how reliable the data received is.

iii. Properly checking that the files are relevant to avoid rewarding a peer for irrelevant files.

After the validation checks, a block is formed and stored in the record module. The system workflow is given in Figures 2 and 3, the activity diagram with information about the hash value exchange. The algorithm of the proposed system is given in Algorithm 1.

Algorithm 1:Proposed System Algorithm.

1. Start process
2. Open dashboard
3. Select a file to upload
4. Encrypt file
5. Share files with peers in the Network
6. If (Shared files is valid) {
7. Link hash values
8. Consensus by all peers in the Network
9. All peers append validation and store the block
10. } else {
11. The message "Files Tampered"
12. }
13. End process

IMPLEMENTATION AND EVALUATION

The system performance is evaluated using several blocked peers, the blockchain formed, and the fairness index. It was implemented using an ArrayList and a linked list, and the simulation and hash values associated with each child peer are based on randomness.

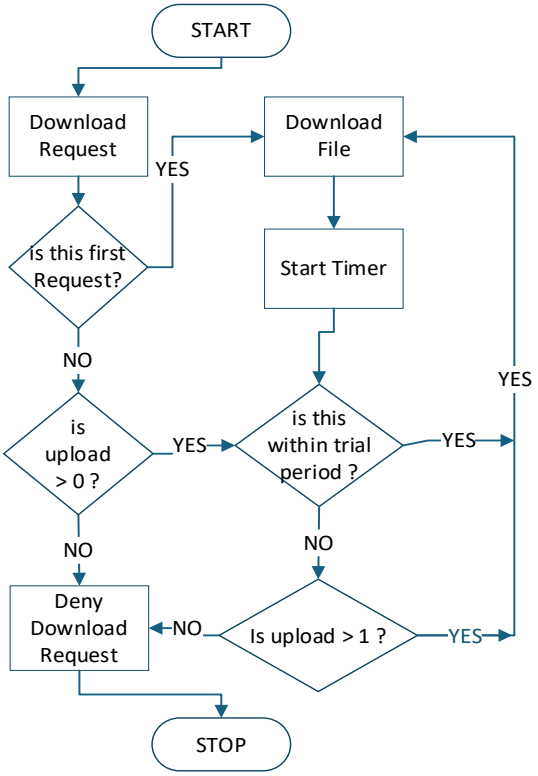


Figure 2: System flowchart

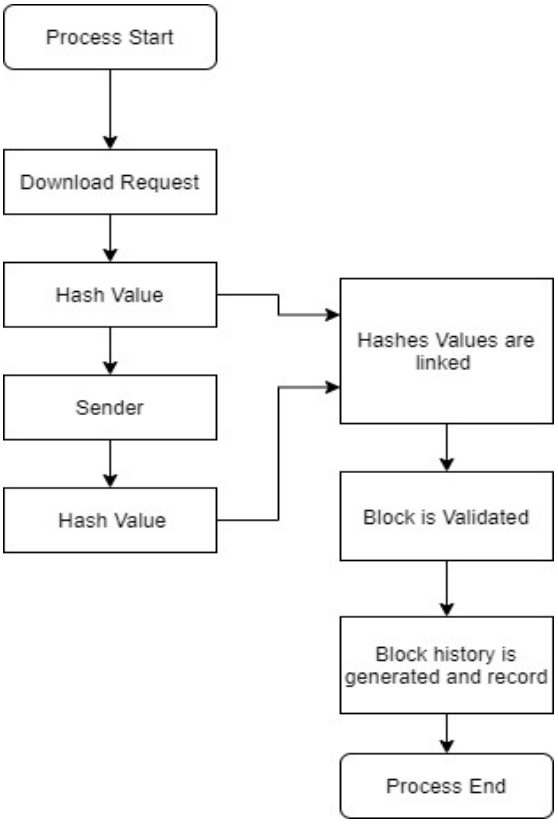


Figure 3: System activity diagram with the hash value exchange

Fairness: Fairness is a key metric in P2P networks, which measures how peers distribute resources by uploading and downloading. When the fairness index approaches 1, it indicates that each peer contributes roughly as much as it consumes, fostering cooperation and stability within the network.

The result of the fairness index, as shown in Figure 4, revealed values ranging from 0.8 to 0.9. The index starts high, around 0.9 with 500 peers, and slightly decreases to about 0.81 with 1000 peers. Beyond this point, the fairness index remains relatively stable as the network expands to 2500 peers. Overall, the system is fairly equitable, though a slight decline is observed.

These findings suggest that the proposed blockchain-based incentive mechanism effectively reduces free-riding and promotes balanced resource sharing among peers. The approach enables activity tracking and verification for each peer, helping to ensure fair contributions without relying solely on trust. This method outperforms traditional P2P networks by maintaining higher fairness levels. The results confirm that integrating blockchain into P2P systems can support fairness in large-scale networks.

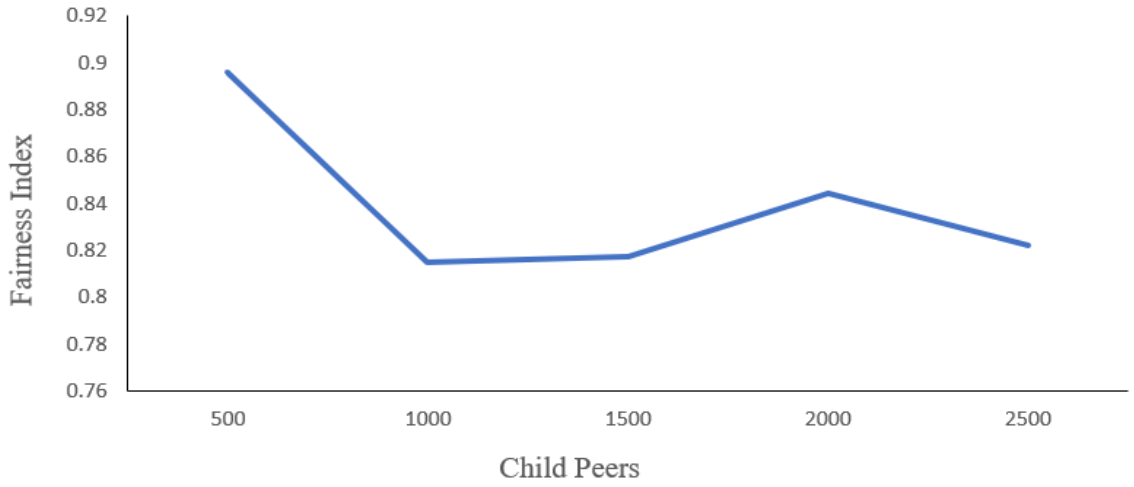


Figure 4: Fairness index graph

Number of blockchains formed: child peers in the network with a hash value linked appropriately and accurately to other child peers forming a unique chain. The blockchain links each request or download with the hash value of the upload or sender hash values after validation, and forms a chain with an immutable record**.** Figure 5 shows the number of blocks formed in the blockchain as the number of child peers in the network increases. The results indicate a steady rise in the number of blocks, growing from around 1000 when there are 500 peers to nearly 4500 when the network scales to 2500 peers. This trend pattern signifies that as more peers connect to this network and upload and download, the system effectively forms more blocks to capture such activities. The outcomes demonstrate the scalability of the suggested approach and the potential of handling the increasing number of exchanges with peers.

The greater number of blocks created emphasises that the system accurately monitors each peer's uploads and downloads through unique hash values. These hash values ensure that every activity is correctly linked and verifiable, supporting fairness and accountability within the network. By relying on hash values for connection and validation, the proposed framework improves the reliability of

records in peer-to-peer environments. Blocked peers are identified as free riders and are therefore excluded from validation and not added to the list of validated blocks. The simulation results of the blocked peers as displayed in Figure 6. The results showed that the number of blocked peers increases as several peers join the network; this indicates that the scheme is capable of managing free riders in the network. The figure reveals a clear upward trend: as the number of child peers grows from 500 to 2500, the number of blocked peers rises steadily, reaching nearly 400. The more peers, the more likely it is that some peers will want to consume without contributing, resulting in free-riding behaviour. The findings confirm the success of the proposed blockchain-based scheme to detect and isolate non-contributing peers; blocking free riders preserves fairness and ensures that resources are shared more equitably among participating peers.

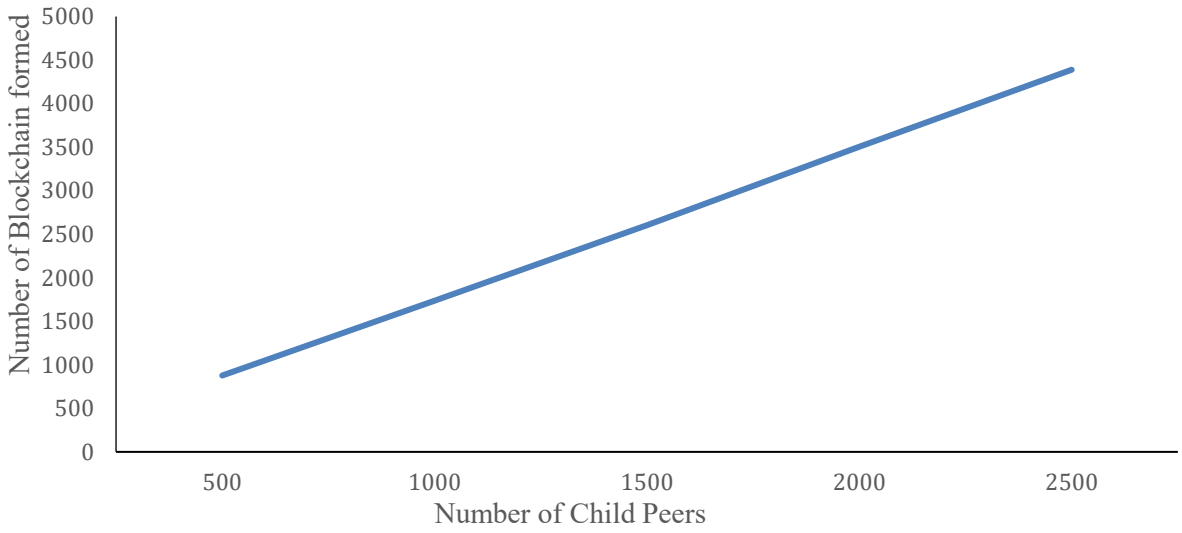


Figure 5: Blockchain formed

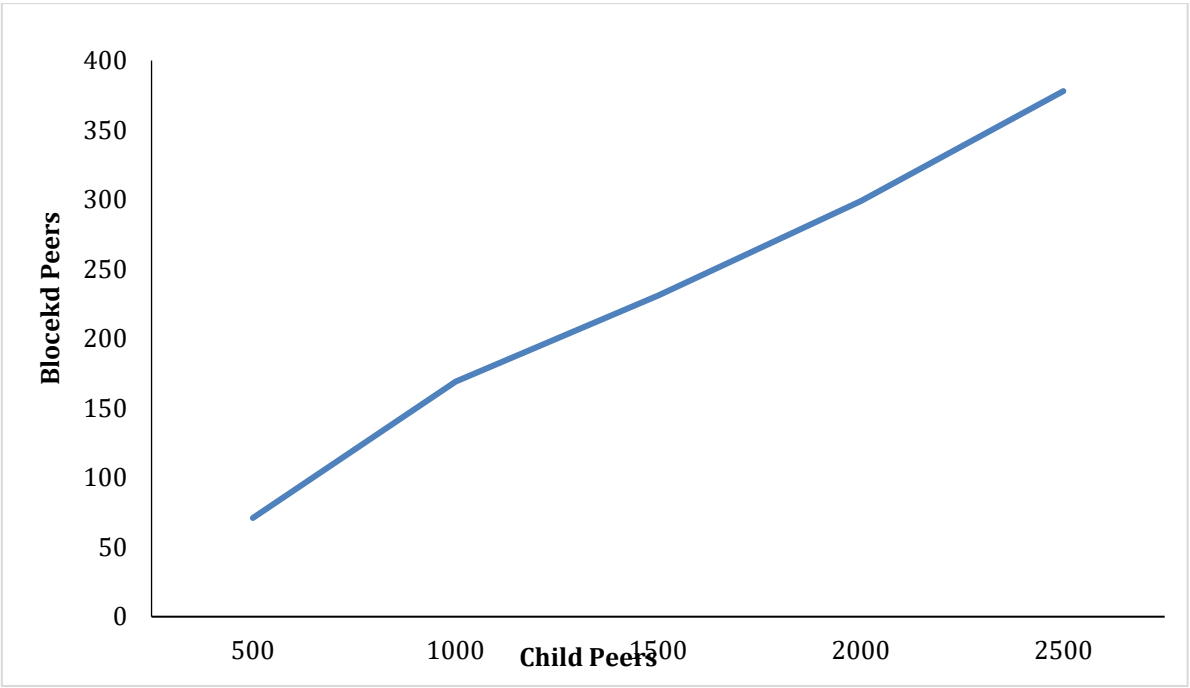


Figure 6: Blocked peers

The results reveal that the proposed approach scales effectively without losing its ability to identify and manage the free-riding behaviour with an increase in the size of the network.

CONCLUSION

In this study, a security mechanism for alleviating free-riding in a peer-to-peer network is designed. The system employs the features of blockchain technology to prevent free-riders in large-scale dynamic networks and maximise effective resource sharing in a mesh overlay topology. In addition, the framework shows that utilising encrypted hash values unique to each peer makes tracking, record keeping, and easy identification of free-riding a maintainable strategy. The system is tested using a file-sharing system and simulated using JAVA programming language while mimicking different peers' simulation scenarios by simulating various types of peer behaviours or roles in the network to see how the system performs under different conditions. The simulation results showed that the system is robust and efficient in tackling free-riding attacks on the Internet. In future work, the scheme will be extended and evaluated using video and audio trace files to assess its performance in handling high-bandwidth, real-time data scenarios.

REFERENCES

Alotibi, B., Alarifi, N., Abdulghani, M., nd Altoaimy, L. (2019). Overcoming free-riding behaviour in peer-to-peer networks using a points system approach. *Procedia Computer Science*, *151*, 1060-1065., 1060-1065.

Biaou, B. O. S., Oluwatope, A. O., Odukoya, H. O., Babalola, A., Ojo, O. E., and Sossou, E. H. (2020). Ayo game approach to mitigate free riding in peer-to-peer networks. *Journal of King Saud University-Computer and Information Sciences*.

Edirimannage, S., Khalil, I., Elvitigala, C., Daluwatta, W., Wijesekera, P., and Zomaya, A. Y. (2025), ZeTFRi - A Zero Trust-Based Free Rider Detection Framework for Next Generation Federated Learning Networks, in IEEE Journal on Selected Areas in Communications, doi: 10.1109/JSAC.2025.3560013.

Huang, S., Wang, G., Yan, Y., and Fang, X. (2020). Blockchain-based data management for digital twin of product. *Journal of Manufacturing Systems*, *54*, 361-371.

Huang, X., Ye, D., Yu, R., and Shu, L. (2020). Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. *IEEE/CAA Journal of Automatica Sinica*, *7*(2), 426-441.

Jafari N., N., Sharifi Milani, F. A. (2015). Comprehensive study of the resource discovery techniques in Peer-to-Peer networks. *Peer-to-Peer Netw. Appl.* **8,** 474–492 https://doi.org/10.1007/s12083-014-0271-5.

Kurdi, H., Althnian, A., Abdulghani, M., and Alkharji, S. (2020). An Adjusted Free-Market-Inspired Approach to Mitigate Free-Riding Behavior in Peer-to-Peer Fog Computing. Electronics, 9(12), 2027.

Ramaswamy, L. and L. Liu, L. (2003). Free riding: a new challenge to Peer-to-Peer file sharing systems. Proceedings of the 36th Hawaii International Conference on System Sciences. Hawaii, 220–229

Li X., He Q., Jiang B., Qin X., Qin K. (2020) BTS-PD: A Blockchain Based Traceability System for P2P Distribution. In: Zheng Z., Dai HN., Tang M., Chen X. (eds) Blockchain and Trustworthy Systems. BlockSys 2019. Communications in Computer and Information Science, 1156. Springer, Singapore. https://doi.org/10.1007/978-981-15-2777-7_50.

Liu L., and Antonopoulos N. (2010) From Client-Server to P2P Networking. In: Shen X., Yu H., Buford J., Akon M. (eds) Handbook of Peer-to-Peer Networking. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-09751-0_3.

Ma, R. T., Lee, S. C., Lui, J. C., & Yau, D. K. (2006). Incentive and service differentiation in P2P networks: A game theoretic approach. Ieee/ACM Transactions on networking, 14(5), 978-991.

Masinde, N., and Graffi, K.(2020). Peer-to-Peer-Based Social Networks: A Comprehensive Survey. *SN COMPUT. SCI.* **1,** 299 https://doi.org/10.1007/s42979-020-00315-8

Musa, A., Abubakar, A., Gimba, U. A., and and Rasheed, R. A. (2019). An Investigation into Peer-to-Peer Network Security Using Wireshark. In *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)* (pp. 1-6). IEEE.

Ojo, O. E., Iyadi, C. O., Oluwatope, A. O., and Akinwale, A. T. (2020). AyoPeer: The adapted ayo-game for minimizing free riding in peer-assisted network. *Peer-to-Peer Networking and Applications*, *13*(5), 1672-1687.

Padhy, R. P., and Patra, M. R. (2012). Evolution of cloud computing and enabling technologies. *International Journal of Cloud Computing and Services Science*, *1*(4), 182.

Putz, B., Dietz, M., Empl, P., & Pernul, G. (2021). Ethertwin: Blockchain-based secure digital twin information management. Information processing & management, 58(1), 102425.

Rahmadika, S., and Rhee, K. H. (2018). Blockchain technology for providing an architecture model of decentralized personal health information. *International Journal of Engineering Business Management*, *10*, 1847979018790589.

Raza, A., Jingzhao, L., Adnan, M., & Ahmad, I. (2024). Optimal load forecasting and scheduling strategies for smart homes peer-to-peer energy networks: A comprehensive survey with critical simulation analysis. Results in Engineering, 22, 102188.

Ripeanu, M. (2001). Peer-to-peer architecture case study: Gnutella network. *In Proceedings first international conference on peer-to-peer computing* (pp. 99-100). IEEE.

Rowaihy, H., Enck, W., McDaniel, P., and La Porta, T. (2005). Limiting sybil attacks in structured peer-to-peer networks, Technical report, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, USA.

Shareh, M. B., Navidi, H., Javadi, H. H. S., and HosseinZadeh, M. (2019). Preventing Sybil attacks in P2P file sharing networks based on the evolutionary game model. *Information Sciences*, *470*, 94-108.

Tian, G., Duan, Z., Baumeister, T., & Dong, Y. (2014). Reroute on loop in anonymous peer-to-peer content sharing networks. In 2014 IEEE Conference on Communications and Network Security (pp. 409-417). IEEE.

Vimal, S., and Srivatsa, S. K. (2020). A new cluster P2P file sharing system based on IPFS and blockchain technology. *Journal of Ambient Intelligence and Humanized Computing*, 1-7.

Vivekanadam, B. (2020). Analysis of recent trend and applications in blockchain technology. *Journal of ISMAC*, *2*(04), 200-206.

Wang, M., Xu, C., Chen, X., Zhong, L., Wu, Z., and Wu, D. O. (2020). BC-Mobile Device Cloud: A Blockchain-Based Decentralized Truthful Framework for Mobile Device Cloud. *IEEE Transactions on Industrial Informatics*, *17*(2), 1208-1219.

Yousafzai, A., Kumar, P. M., and Hong, C. S. (2021). CROWD-CDN: A cryptocurrency incentivized crowdsourced peer-to-peer content delivery framework. *Computer Communications*, *179*, 260-271.

Yijiao, Y. and Jin Hai, J. (2008). A survey on overcoming free riding in Peer-to-Peer networks. Chinese Journal of Computers, 31(1), 1–15.