ISSN: 2395-7852

# International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 2, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

# A Transatlantic Approach Consortium Blockchain Architecture Based Digital Currency System

**S.SHALINI, Ms.GEETHA**

II MCA, Department of MCA, Paavai Engineering College, Paavai Nagar, Pachal, Tamilnadu, India

Professor, Department of MCA, Paavai Engineering College, Paavai Nagar, Pachal, Tamilnadu, India

**ABSTRACT**: In the big data environment, data are characterized by a large volume, various types, and rapid changes. The consortium blockchain applied in this environment faces the problem of excessive storage of the ledger, and the ledger handling different types of business needs to be isolated to ensure the ledger's security. To this end, this paper proposes a scalable consortium blockchain architecture based on world state collaborative storage (CBCS). First, a business world state database update method is designed based on sparse Merkle multiproofs, where the collaborative storage of world state is realized under the premise of mutual isolation of the ledger between business domains. Then, a world state consistency verification method based on the rank B+ tree is designed to verify the consistency of the business world state in business domains by the checking sidechain, and a main-side chain cross-anchoring structure is designed to realize secure anchoring of the mainchain and the checking sidechain. Meanwhile, a blockchain transaction trusted tracing method based on two-level certification is developed to enable business nodes to obtain complete blockchain transactions. Finally, the feasibility and efficiency of the proposed mechanism to solve the storage scalability problem in the consortium blockchain are verified through experiments.

## I. INTRODUCTION

The current research on the scalability of blockchain storage mainly focuses on the processing of blocks in the chained ledger but ignores the critical role of the state database. The chained ledger ensures the security of a block by connecting it with its front and back blocks. Since the chained ledger is stored in the form of files and direct access to the blockchain transactions in it requires searching the block files one by one, which is inefficient. The world state database contains critical data extracted from the chained ledger and stores the latest values of the world state in the form of key-value pairs. Owing to its characteristics of high value, a small storage space occupation, high query efficiency, and fine-grained slicing, the world state database occupies an important position in the consortium blockchain system. In practice, we can retrieve the required ledger data by searching the world state database, thus satisfying most of the application requirements in the consortium blockchain system. Chen et al. [10] proposed a high-performance consortium blockchain storage architecture for a big data environment. In this architecture, the consortium blockchain ledger is divided into continuous data and state data, an index-based method and a multi-level cache method are designed to process continuous data and state data, respectively. However, this scheme focuses on improving the read–write performance of the ledger but does not address the scalability issue of the consortium blockchain ledger storage.

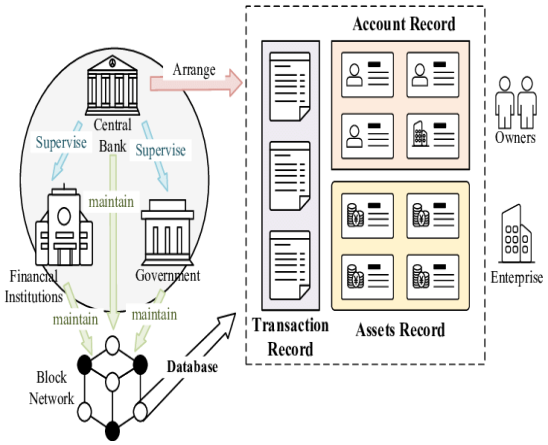



Fig 1: Digital currency scheme

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

Meanwhile, in existing application scenarios, a consortium blockchain system often has the need to process blockchain transactions of multiple business scenarios simultaneously, in which the ledger data need to be isolated to enhance ledger security. Hyperledger fabric [11], an open-source platform for consortium blockchain, uses channel technology to realize the processing in different scenarios. In each business scenario, its ledger is processed and recorded through a separate channel. However, the organizations joining multiple channels need to store the ledger of multiple channels in the blockchain nodes, which increases the pressure on the blockchain nodes to store the ledger.

This paper focuses on the world state data in the consortium blockchain ledger. According to different business types, the complete world state database is divided into different business world state databases. Then, the consortium blockchain nodes of different business departments process different business world state to realize collaborative storage of the world state database. In this way, the storage space of the consortium blockchain node can be efficiently saved, and the ledger data in different business scenarios can be isolated safely. Collaborative storage is a common approach for solving the storage scalability problems of blockchain [12]. However, the existing studies mostly use random or sequential order of transactions to divide the chained ledger into different pieces and store them in different blockchain nodes, which increase the communication and time costs of acquiring the local unstored ledger data. The world state data are in the form of a single key-value pair, which has a smaller granularity than the chained ledger. By dividing the world state database according to different business scenarios, the consortium blockchain node can store the world state data most frequently used in its business, thus effectively improving the efficiency of querying ledger data.

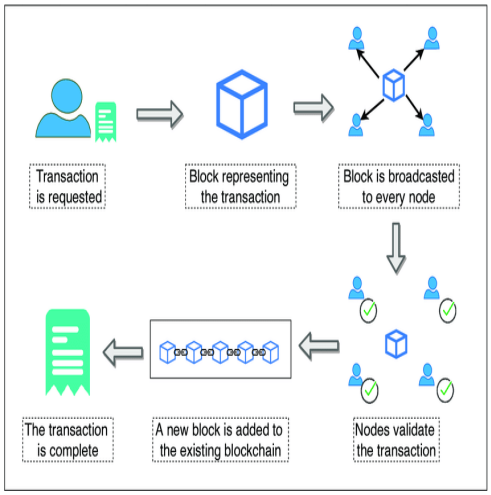



Fig 2: Working Of Blockchain

In addition, this paper fully considers the security of the world state data. The world state in the consortium blockchain can improve the accessing speed of the ledger data and serve as a basis for determining the validity of the read–write sets of blockchain transactions. Moreover, it can update and read the world state through write operation and read operation, respectively, but there are big differences in the execution process of the two kinds of operations. When a blockchain transaction is initiated to perform a write operation to the ledger, an endorsement policy can be set up to stipulate that the blockchain transaction can only write new data to the blockchain ledger after it has been verified by enough organizations. However, when a blockchain transaction is initiated to read the world state, the endorsement of multiple organizations is not required. The blockchain node obtains the corresponding state data through the locally stored world state database and returns it to the applicant. After completing the write operation, the world state database has a high independence degree, which is less secure than the chained ledger stored through the chained structure, especially for those scenarios where data management is not strict or other security issues exist. If the data stored in the world state database are corrupted or maliciously modified, the operation of reading the world state has the risk of returning non-trusted data [13]. In our study, the consistency of the state data is periodically verified to ensure the security of the business world state databases stored by the consortium blockchain nodes.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

## II. RELATED WORK

At present, many scholars have researched the blockchain storage scalability problem from different perspectives for different application scenarios, and the methods can be classified into the off-chain storage-based method and the on-chain storage-based method.

The off-chain storage-based method transfers the storage pressure of the ledger to off-chain storage resources, such as cloud storage [14], distributed storage system IPFS (InterPlanetary File System) [15], etc. On-chain nodes store only the metadata of the ledger (including off-chain storage addresses, hash values of transaction data, etc.) to reduce storage pressure. Zheng et al. [16] proposed to store blockchain transactions generated by miner nodes in the IPFS network, and pack the storage addresses of transactions returned by the IPFS network instead of the original blockchain transactions into blocks for storage, using the feature that the storage address occupies less storage space to save the on-chain storage space. He et al. [17] provided the Chameleon architecture. In this architecture, the complete ledger data are stored on the cloud storage system, and the blockchain nodes only store the ledger of the most recent period. Xu et al. [18] proposed SlimChain, where the off-chain nodes store some or all ledger data according to their storage capacity and verify the validity of transactions. The on-chain nodes only store part of the block header data such as the transaction hash and the previous block hash, and based on this, the validity of the ledger data stored by the off-chain nodes can be verified. The above methods of transferring the ledger to off-chain storage space can dynamically adjust the demand for off-chain storage space with the change in ledger volume. However, these methods reduce the decentralization of the blockchain system, and it is necessary to ensure the off-chain ledger storage security to prevent the ledger from being destroyed.

In the on-chain storage-based method, all the ledger data are stored in the blockchain nodes. The on-chain storage-based method can be further divided into the light node-based method and the collaborative storage-based method.

The light node-based method is widely used in cryptocurrency wallets [19] or Internet of Things (IoT) [20] scenarios to solve the problem that the weak storage capacity of terminal nodes is not suitable for storing larger-scale blockchain ledger. For blockchain systems using the unspent transaction outputs (UTXO) model [21], Palai et al. [22] proposed the block summarization method, which merges the inputs and outputs of transactions in adjacent blocks to generate the summarized blocks. Then, these blocks are stored on resource-constrained light nodes, enabling the light nodes to verify blockchain transactions independently. However, this method can only be applied to blockchain systems using the UTXO model, and it is not suitable for blockchain systems that deploy smart contracts. In blockchain-based IoT applications, IoT nodes often have limited storage resources. To address this issue, Kim et al. [23] proposed the storage compression consensus (SCC) algorithm, which improves the practical Byzantine fault tolerance (PBFT) consensus algorithm [24] to increase the block compression process. In this algorithm, the Merkle tree is constructed by calculating the hash of the existing blocks, and the root node of the Merkle tree is recorded in the compressed blocks. After the end of the consensus cycle, the IoT nodes with limited storage resources store the compressed blocks and the latest blocks, and delete the blocks stored in the previous cycle. In this method, the IoT nodes need to rely on the full node to extract the blockchain transactions in the compressed blocks, which reduces the decentralization of the blockchain system and increases time consumption in requesting blockchain transactions. Liu et al. [25] designed an irrelevant block filtering method to filter the blocks that cannot be invoked by subsequent blockchain transactions according to the actual application scenario of industrial IoT. The dynamic storage nodes only store the useful blocks that can be invoked subsequently. However, this method is closely related to the actual application scenario and is not suitable for the scenario where all existing blocks are likely to be invoked by subsequent transactions.

## III. METHODS

Consortium Blockchain

Consortium blockchain is a kind of blockchain technology specially developed for enterprises or other groups to realize trusted distributed data processing. Unlike Bitcoin, which is oriented to the field of cryptocurrency, there is no need for miners to mine in the consortium blockchain, and no cryptocurrency is generated. The consortium blockchain achieves consensus through consensus algorithms such as PBFT, which run by voting, consume less energy and computing resources, and can reduce the delay of consensus.

Consortium blockchain consists of different organizations. Each organization is a group of different types of nodes. The consortium blockchain carries out strict authentication and permission management on nodes, and the ledger data can only be accessed by nodes in the organization, thus isolating ledger data from external nodes. The submitting nodes in the consortium blockchain initiate blockchain transactions through chaincodes, and the blockchain transactions are formed into blocks through the ordering service after endorsement. These blocks are linked back and

forth to form a chained ledger. Meanwhile, the world state is generated and stored as a key-value pair (*key*, *value*). The *key* identifies the world state, and the *value* records the version *rev* of the world state and other data related to specific business scenario. The chaincode of the consortium blockchain contains several smart contracts [35], which enable the creation, query, and update of the world state. When the world state is updated, the *key* is kept unchanged, and the version *rev* and other data related to the specific business scenario are updated.

The ledger stored by the consortium blockchain nodes includes a history database as well as an index database in addition to the chained ledger and the world state database. The history database stores the information of blockchain transactions that update the world state data database. The index database holds the locations of the blocks in the file where the chained ledger is stored.

In this case, the master node and business nodes use different ledger storage strategies. To guarantee that the ledger is fully available in the organization, the master node stores all ledger of consortium blockchain, including the chained ledger, the world state database, the history database, the index database and the checking sidechain proposed in our scheme. However, the master node does not increase the management privileges to the business nodes, and the business nodes still operate in a decentralized manner. A master node is set up in each organization, and all master nodes form the master domain. The business nodes in the same organization are responsible for different businesses, and the business nodes responsible for the same business in different organizations form a business domain. The business nodes in the same business domain handle the same business based on the same business chaincode and maintain a consistent business world state database. Meanwhile, the business node stores the business world state database in the business domain to which it belongs, and the block headers of the checking sidechain. The business world state database is a class of data in the complete world state database for handling the same business, and the business world state database in a business domain is generated by the same chaincode.

Business World State Database Update

After the business node obtains the business block, the block header of the complete block, and $Amount_{list}$, the authenticity of the blockchain transactions in the business block need to be verified. First, it is verified whether the block number recorded in the business block header matches the block number recorded in the complete block header to ensure that the business block matches the complete block. Then, it is verified whether the number of entries recorded in $Amount_{list}$ is consistent with the actual number of blockchain transactions contained in the business block. Finally, a layer-by-layer verification approach is designed, and the multiproofs auxiliary information is used to prove the existence of the blockchain transactions obtained from the business block in the complete block.

The hash of the blockchain transactions in the business block is calculated as *merkle_value* of the node at the bottom of the Merkle tree, and *merkle_key* corresponding to each *merkle_value* is obtained, where the superscript $i$ is 0, the subscript $j$ is the serial number of each blockchain transaction in the complete block. The obtained node is recorded at *Merkle_level0*, i.e., the 0th level of the Merkle tree.

To avoid affecting the generation of blockchain transactions in the mainchain, the consistency of business world state data cannot be verified by initiating blockchain transactions in the mainchain. To address this issue, this paper sets the checking sidechain and then initiates checking transactions in the checking sidechain to achieve consensus on the consistency information of the business world state database. Meanwhile, the main-side chain cross-anchoring structure is proposed, which uses a two-way recording of the mainchain and the checking sidechain to achieve information matching and improve the security of the checking sidechain.

## IV. RESULT ANALYSIS

This study generates business blocks through the ordering service. The ordering service is a decentralized consensus module in the consortium blockchain, which ensures the reliability of operation by executing the system chaincodes. The ordering service connects with business docking nodes in each business domain and distributes the business blocks. The distribution of business blocks does not rely on central agency, which ensures that the business block distribution process is highly decentralized.

The business nodes in the same business domain receive $Amount_{list}$ and the block header of the complete block from the organizations they belong to. The business nodes do not need to maintain complete trust in the business docking node in this business domain. They can verify whether the account of the blockchain transactions in the business block is consistent with the $Amount_{list}$ to prevent blockchain transactions in the business block from being maliciously deleted; meanwhile, they use the received multiproofs auxiliary information and the blockchain transactions in the business block to calculate the root node of the sparse Merkle multiproofs. Then, they compare the

hash recorded in this root node with the block body hash recorded in the complete block header to ensure the authenticity of the blockchain transactions in the business block. When a business node in the business domain finds that the business block received from the business docking node does not correctly match, it can agree with other business nodes in the business domain on the reason for the unmatch and then determines whether the behavior of the business docking node is trustworthy. If the business docking node is found to have untrustworthy behaviors, it is replaced and penalized.

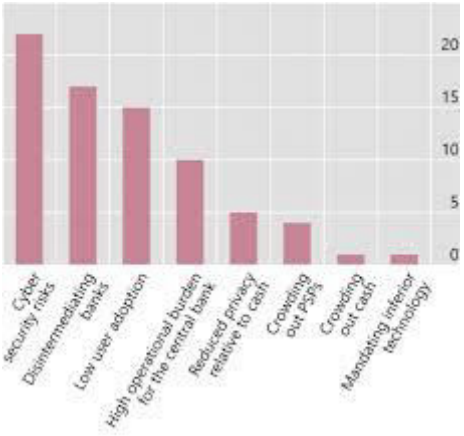



Fig 3: Result analysis

The business nodes can exploit the blockchain transactions in the verified business blocks to update their respective business world state databases, keeping the ledger synchronized with the mainchain. According to the business world state database, the business node can verify the legitimacy of the read–write sets in the blockchain transactions, and only the blockchain transactions containing the legal read–write sets can update the world state data. In this process, the business node does not need to access the ledger in other business domains, thus realizing security isolation of the ledger and ensuring controlled access to the ledger while ensuring a high decentralization degree.

## V. CONCLUSIONS

This paper proposes a scalable consortium blockchain architecture based on world state collaborative storage. In this architecture, the business nodes collaboratively store the world state database to effectively reduce the pressure of ledger storage and isolate the ledger data between different business domains. The consistency of the business world state stored by the business nodes can be verified by initiating consistency verification transactions through the checking sidechain. The proposed scheme can effectively save the ledger storage space of the consortium blockchain nodes while ensuring a high decentralization degree and retrieval efficiency of the ledger data. Meanwhile, the structure design of the scheme has a high similarity with the internal organizational structure of the social organization or group, which is convenient for the actual deployment in the social organization or group. It is important to note that the checking height threshold $c$ in our scheme determines the time interval between two consistency checkings, which affects both the timeliness of discovering world state data corruption and the computational overhead of consistency checkings. It is necessary to set the checking height threshold $c$ according to different needs in different application scenarios. In the future, we will apply our designed scheme to projects related to specific scenarios such as big data sharing, and conduct a more detailed evaluation of the practical application effect of the scheme.

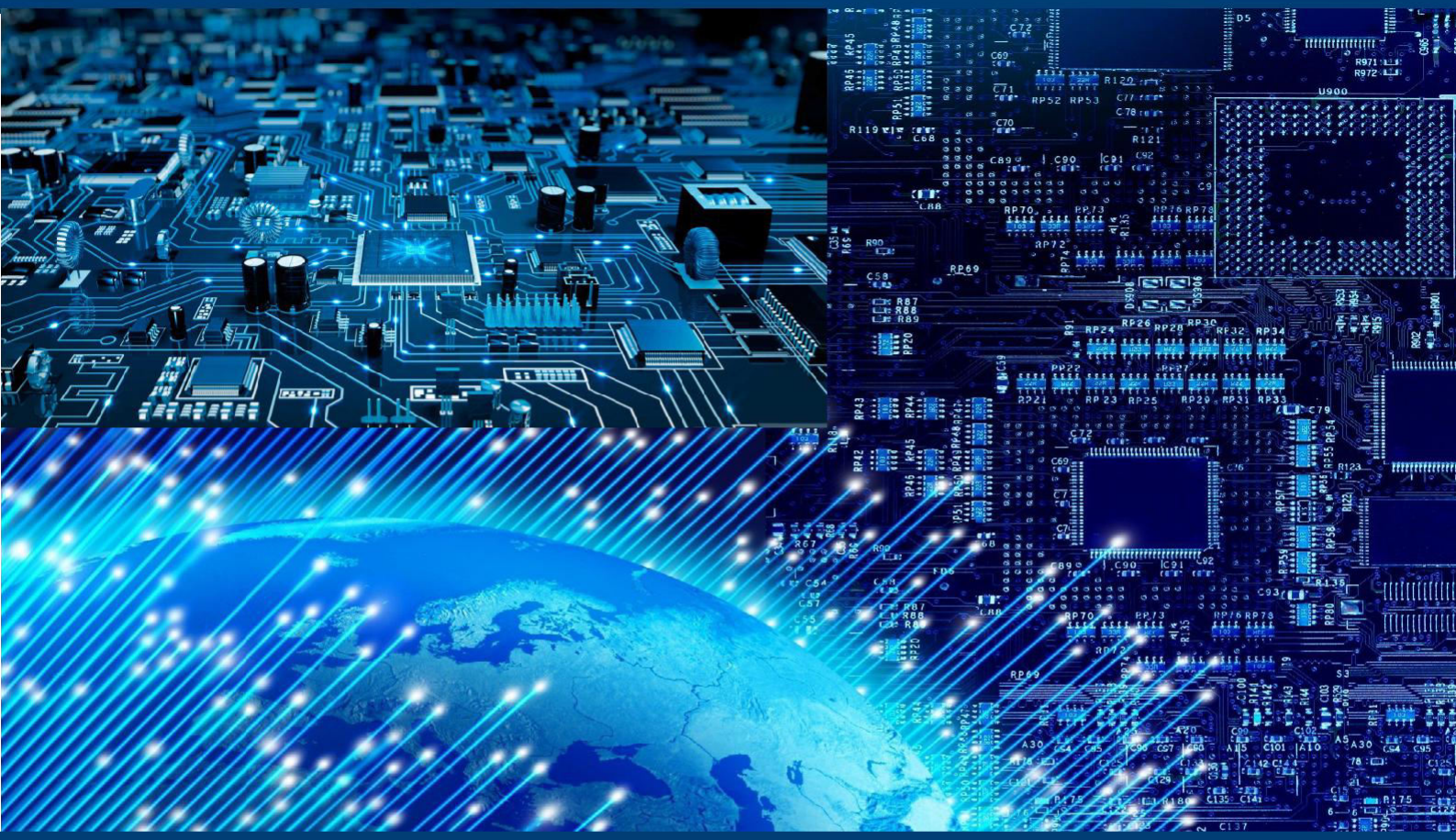
## REFERENCES

1. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A survey on blockchain for information systems management and security. *Inf. Process. Manag.* **2021**, *58*, 102397. [Google Scholar] [CrossRef]
2. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: **https://bitcoin.org/bitcoin.pdf** (accessed on 16 September 2022).
3. Sun, Z.; Zhang, X.; Xiang, F.; Chen, L. Survey of storage scalability on blockchain. *J. Softw.* **2021**, *32*, 1–20. [Google Scholar]
4. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [Google Scholar] [CrossRef]
5. Dib, O.; Brousmiche, K.L.; Durand, A.; Thea, E.; Hamida, E.B. Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun.* **2018**, *11*, 51–64. [Google Scholar]

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

6. Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. FastFabric: Scaling hyperledger fabric to 20,000 transactions per second. *Int. J. Netw. Manag.* **2020**, *30*, e2099. [Google Scholar] [CrossRef]
7. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 1–18. [Google Scholar] [CrossRef] [PubMed]
8. Gao, Z.; Cao, L.; Du, X. Data right confirmation mechanism based on blockchain and locality sensitive hashing. In Proceedings of the 2020 3rd International Conference on Hot Informationcentric Networking (HotICN), Hefei, China, 12–14 December 2020. [Google Scholar]
9. Nyaletey, E.; Parizi, R.M.; Zhang, Q.; Choo, K.K.R. BlockIPFS-blockchain-enabled interplanetary file system for forensic and trusted data traceability. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019. [Google Scholar]
10. Chen, X.; Zhang, K.; Liang, X.; Qiu, W.; Zhang, Z.; Tu, D. HyperBSA: A high-performance consortium blockchain storage architecture for massive data. *IEEE Access.* **2020**, *8*, 178402–178413. [Google Scholar] [CrossRef]
11. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Yellick, J. Hyperledger fabric: A distributed op-erating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018. [Google Scholar]
12. Yu, G.; Wang, X.; Yu, K.; Ni, W.; Zhang, J.A.; Liu, R.P. Survey: Sharding in blockchains. *IEEE Access* **2020**, *8*, 14155–14181. [Google Scholar] [CrossRef]
13. Gao, Z.; Zhang, D.; Zhang, J. A security problem caused by the state database in Hyperledger Fabric. In Proceedings of the International Conference on Frontiers in Cyber Security, Tianjin, China, 15–17 November 2020; pp. 361–372. [Google Scholar]
14. Sharma, P.; Jindal, R.; Borah, M.D. Blockchain technology for cloud storage: A systematic literature review. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–32. [Google Scholar] [CrossRef]
15. Benet, J. Ipfs-Content Addressed, Versioned, p2p File System. Available online: **https://arxiv.org/abs/1407.3561** (accessed on 16 September 2022).
16. Zheng, Q.; Li, Y.; Chen, P.; Dong, X. An innovative IPFS-based storage model for blockchain. In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, 3–6 December 2018; pp. 704–708. [Google Scholar]
17. He, G.; Su, W.; Gao, S. Chameleon: A scalable and adaptive permissioned blockchain architecture. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 87–93. [Google Scholar]




# International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)



| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |