IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 20 December 2022, accepted 13 January 2023, date of publication 27 January 2023, date of current version 6 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3240237

SURVEY

A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks

MUHAMMAD IRFAN KHALID[1], IBTISAM EHSAN[2], AYMAN KHALLEL AL-ANI[3], JAWAID IQBAL[4], SADDAM HUSSAIN[5,6], SYED SAJID ULLAH[7,8], AND NAYAB[9]

[1]Department of Information and Electrical Engineering and Applied Mathematics, University of Salerno, 84084 Fisciano, Italy
[2]Department of Information Technology, University of Sialkot, Sialkot 51040, Pakistan
[3]Network Engineering, Faculty of Computing and Informatics (FCI), Universiti Malaysia Sabah, Kota Kinabalu, Sabah, Malaysia
[4]Department of Computer Science, Capital University of Science and Technology, Islamabad 44000, Pakistan
[5]Department of Computer Science and Information Technology, Hazara University Mansehra, Dhodial 21120, Pakistan
[6]School of Digital Science, Universiti Brunei Darussalam, Jalan Tungku Link, Gadong BE1410, Brunei
[7]Department of Information and Communication Technology, University of Agder (UiA), 4898 Grimstad, Norway
[8]Department of Electrical and Computer Engineering, Villanova University, Villanova, PA 19085, USA
[9]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan

Corresponding authors: Ayman Khallel Al-Ani (ayman@ums.edu.my) and Saddam Hussain (saddamicup1993@gmail.com)

This work was supported by the Research Management Centre (RMC), Universiti Malaysia Sabah.

ABSTRACT Blockchains are a new approach to creating distributed networks that were first introduced in 2008. It allows the formation of peer-to-peer networks based on consensus, forming chains from accepted blocks without requiring a central authority or centralized controller. A prominent application of this technology is its use in decentralized storage systems. Individuals in decentralized storage networks rent unused hardware storage space to other individuals. A decentralized network utilizing end-to-end encryption eliminates the risk of data loss associated with centralized data control by enabling clients to transmit their files securely. The storage providers must prove that they have kept unaltered files in this network for this time. Many studies have been conducted in this specific domain, most targeting storage capacity and efficiency, but a security, integrity and privacy loophole need to be addressed. This paper presents an overview of blockchain-based storage systems and how they work, followed by a comparison with cloud-based storage networks and a survey of various decentralized storage networks like SIA, File coin, and Storj available on the market. Next, we discuss the advantages and disadvantages of blockchain-based storage. In our final discussion, we examine the security problems of decentralized storage networks and explore potential solutions and research directions for the future.

INDEX TERMS Decentralized storage, blockchain, storage networks, blockchain storage.

I. INTRODUCTION

In recent years, technological developments within the field of blockchain technology have caused us to question our perception of the internet as a network of centralized service providers. Decentralized ledgers have proved their importance to various blockchain networks. Platforms like these decentralized networks allow anyone to build valuable services without centralized management. Blockchain technology is used across many applications, including financial transactions, supply chain systems, and social networking. In addition to producing a large amount of data daily, computers, smartphones, and cameras require a growing amount of space to store that data [1]. A cloud storage system was created to meet this need. Providing storage services, the Cloud is a cooperative system comprising multiple devices, multiple applications, and many forms of service. Local storage is more costly, less reliable, and more likely to lose data than cloud storage. Cloud storage refers to storing user data on servers managed by a third party and secured by that third party. The data is stored in remote devices' memory rather than on the owner's hardware. Even though cloud computing presents many security and availability concerns, it represents a significant innovation in computing. Having no visibility or control over stored data is one of the biggest problems with cloud storage [2]. A user's data may be stored, handled, or compromised without their knowledge. There needs to be more trust between users and companies. Users cannot claim

The associate editor coordinating the review of this manuscript and approving it for publication was Mueen Uddin.

compensation because there is no formal contract between them and service providers. In addition, clients need to find out if their data is copied or sold. Nowadays, blockchain technology is widely used in distributed storage systems. Powered by IPFS, Filecoin provides customers and storage miners with an entirely decentralized network of storage services. To initiate transactions, the miner provides the capability of viewing matching quotes within its services. In order to ensure data integrity, a copying proof and space-time certificate are used [3]. The Filecoin protocol includes blockchain records for token transactions, integrity challenge responses, and order books. The Siacoin network allows storage providers and consumers to create smart contracts that allow them to exchange documents. A contract requires customers to submit their data storage certificates during the certification window. If the proof is legal, smart contracts pay the customer's storage provider automatically. A peer-to-peer cloud storage service, Storj, operates on the Storj network. Clients encrypt their files before sending them to the network. By encrypting file blocks, files are protected from unauthorized access. Direct encryption can protect the confidentiality of stored data in distributed storage [4]. Data storage fees are paid by customers after their data provider validates that the data can be recovered. The majority of transaction blocks can be written over an hour after a transaction is released, according to recent analysis. Distributed storage solutions with transaction latency problems do not offer a competitive advantage. Moreover, it shows the importance of updating the system agreement as well as upgrading middlemen to ensure the system's vitality. Furthermore, the block generated by the new protocol node is invalid in the node, which means a hard fork is inevitable. There was a hard fork in Ethereum, and the number has been split into two. In the Ethereum hard fork process, two numbers are created: ETH and ETC Currency. There are some disadvantages to the decentralized system, including slow updating and a difficulty maintaining it. There are a variety of definitions discussed in [5] regarding distributed networks. They share resources such as content, storage, CPU power, and other resources, among others, as one of their main features. A distributed file system has several advantages, including fault tolerance, availability, scalability, and performance. The above benefits can only be achieved by coordinating thousands of servers and executing users' applications tasks. Replicating data increases data availability and reduces data loss in distributed storage file systems. This method is fast and straightforward but poses certain challenges such as large storage overhead. Additionally, multiple data failures need to be avoided by properly distributing files across different domains for replication to be effective [6]. Erasure code is a second method that can solve the problem of huge overheads by reducing computation complexity. In distributed file storage systems, there is no trusted central party to control the network since it is built on blockchain technology. The security of these storage methods is therefore higher than that of other types [7]. Despite recent enhancements to security solutions, it cannot fully fix the Cloud's inherent security flaws. Users can rent out unused space on decentralized blockchain storage networks to other users who need it [4]. Our survey revolves around the use of blockchain technology in storage networks. A decentralized storage network powered by this model allows any computer system with a free disk to participate. In return for lending out this storage, the provider will receive cryptocurrency. Any client that needs free storage can get it from the system [5]. A decentralized ledger stores all the information about available storage, contracts between a client and a provider, and free storage with each provider. This method can develop an autonomous storage network with minimal central control.

A. MOTIVATION AND CONTRIBUTIONS

The importance of decentralized storage networks and their inherent challenges motivates this survey to examine past solutions employed to overcome them. Its key attributes are trust, transparency, and traceability, and blockchain radically transforms the domain [6]. Concerning decentralized storage networks and process decentralization, blockchain technology is a viable candidate for solving the problems related to immutability, integrity, and tamper resistance. This domain has several research gaps concerning data security, privacy, and integrity. An earlier paper [8] in the same field compares blockchain-based storage networks with cloud-based storage networks and presents an overview. Furthermore, different consensus protocols are discussed in each group. Blockchain-based storage systems are discussed in terms of their advantages and disadvantages. However, there are still big research gaps to fill, such as how do decentralize storage systems work? What makes DNS better than cloud storage? Are there any challenges to the adoption of DNS? How DNS is addressing security concerns, as well as the limitations they face. Our research aims to find the best possible solutions to potential problems by conducting a comprehensive survey. Moreover, the highlights of all aspects of decentralized storage will be helpful for researchers in the future. Our research aims to find the best possible solutions to potential problems by conducting a comprehensive survey. Moreover, the highlights of all aspects of decentralized storage will be helpful for researchers in the future.

Our contribution in this paper sums up with the following points.

- Briefly describes the difference between centralized and decentralized storage networks.
- Presents a comprehensive comparison of various storage networks (prize, mostly used, Active nodes, working mechanism, Advantages, Disadvantages, etc.
- Highlights possible attacks and their solutions on decentralized storage systems.
- Presents open challenges and future research direction for decentralized storage networks.

B. PAPER ORGANIZATION

The structure of this paper has three parts. The first part of the paper describes a comprehensive literature search and summarizes the work done so far. The second part outlines existing work on critical subdomains/subfields of decentralized storage systems and reference case studies that have been implemented. In contrast, the third part examines the advantages, disadvantages, limitations, and potential problems associated with decentralized storage. Considering this survey's contribution and novelty, there is a considerable research gap regarding the adoption and security of decentralized storage systems. Many studies have been conducted in this domain, but most focus on aspects other than security and privacy. The comprehensive article compares various storage systems, followed by a discussion of potential security issues surrounding decentralized storage systems and their possible solutions and limitations.

II. RESEARCH METHODOLOGY

Observing the typical patterns in blockchain applications in decentralized storage networks and related domains in the literature is a standard requirement in analyzing previous work. It is intended to identify the applications, challenges, gaps, and future directions of the field. In this way, we identified and collected all literature related to storage, where blockchain was used to solve conventional problems. In each subsection, the findings and issues that were addressed are summarized and tabulated. As a result of this method, potential applications, issues, and challenges that were resolved using blockchain technology in the decentralized domain can be identified. To consolidate the case studies used by non-government and governmental agencies worldwide to solve storage challenges, an exploratory study will be conducted to assess the state-of-the-art implementation of blockchain technology in the decentralized storage domain. Lastly, all the literature was combined to determine the most prevalent applications and current open issues.

A. RESEARCH QUESTIONS

1) What are the potential benefits of blockchain technology in decentralized storage?

2) How can blockchain-based storage applications provide solutions to the issues and challenges identified in decentralized storage and used in previous studies?

3) How can blockchain be deployed for distributed storage networks?

Reports, articles, and review findings about blockchain in decentralized storage networks are discussed in this section as the filters used to narrow down the results. A search of 300 papers produced the initial result. We compiled a list of primary studies based on the criteria applied to preliminary studies. Figure 1 portrays the selection of papers.

B. SEARCH RESULTS

We found five hundred thirty papers using the search strategy (see Figure 4). By removing duplicate papers and applying the study selection process described in Section II-B, 503 papers were excluded. The included papers and the related literature reviews resulted in the addition of four records. Figure 2 displays the paper sorting process.

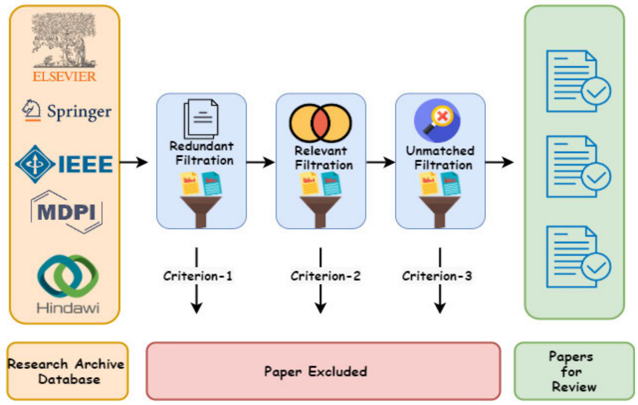


FIGURE 1. Paper selection criteria.

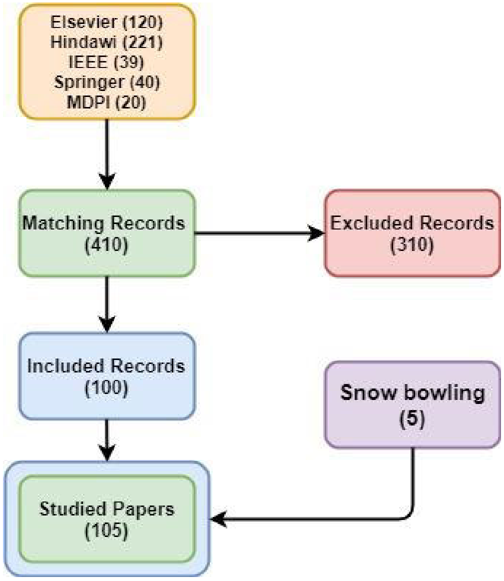


FIGURE 2. Papers sorting.

III. BACKGROUND AND RELATED WORK

Researchers in [7] have analyzed several existing blockchain-based studies. Research in this area indicates that data storage and sharing account for 16% of all research conducted after IoT. The most popular blockchain topics are IoT and data storage. Public and private blockchains aim to resolve the current system's main problems: single points of failure and data tampering. Data can be stored more securely and efficiently using blockchain-based storage networks compared to traditional centralized storage systems that use centralized servers. Among the stored contents are personal information about users, the data of users, or system-related information. The following section examines several proposed ideas that have been made to improve existing blockchain-based storage networks and use blockchain technology to use centralized systems to enhance existing ones. Blockchain-based decentralization Domain Name System (DNS) proposed in [8] can be used to prevent data tampering by storing hashes of zone files. It also has multiple parallel parsing

TABLE 1. Research in decentralized storage networks.

Reference	Paper type	Year	Targeted Domain	Major contribution	Future research directions
[19]	Research	2022	Decentralized Storage Network	It has proposed a mechanism that leverages the smart-contract and oracle network to govern the storage agreement between the client and storage provider efficiently.	Leveraging the smart contract and oracle network to govern the storage contract rules can improve the results' authenticity.
[16]	Review	2021	Decentralized data transfer	Develop prototype systems on top of Ethereum Ropsten using various protocols	To better preserve the digital rights of sold content against pirating consumers, some digital rights management (DRM) schemes can be introduced
[17]	Research	2021	Blockchain-based secure storage	An information compression method for stored data based on double-blockchains was proposed to improve the safety of communication transactions	The proposed system's accuracy can reach 96% with the RSA and DSA algorithms.
[20]	Survey	2021	Decentralized Storage Auditing	The authors proposed an auditing framework for storage that satisfies security and efficiency requirements and outperforms existing approaches.	The data transfer rate and speed can be maximized through discussed mechanisms.
[11]	Research	2021	Blockchain-based Data Storage	To address security challenges, propose consortium blockchain and smart contracts to ensure a trustworthy environment for secure data storage and sharing	A blockchain platform that integrates artificial intelligence (e.g., deep learning) can have a significant impact on the output
[8]	Survey	2020	Decentralized storage networks	A brief survey on decentralized storage networks in terms of security, accuracy, efficiency	Major loopholes in security can be future research perspective
[18]	Research	2020	Verifiable Decentralized Storage	Proposed incremental aggregation as a new notion for Vector Commitment, which allows a bounded number of openings to be merged succinctly	Practical implementation can indicate new loopholes in terms of security
[13]	Research	2020	Data Protection in Blockchain-Based Decentralized Storage Networks	propose a coding scheme for data protection	It is possible to achieve faster recovery speeds with an updated coding scheme compared to an existing network.
[4]	Research	2019	Decentralized Storage Network	The authors studied Task/service allocation in distributed file storage systems.	A smart contract that handles the entire pooling process life cycle, including node management, bidding, verification, and profit sharing
[14]	Research	2018	A decentralized platform for storing and exchanging air-to-ground IoT data	Show how the proposed consensus process for air-to-ground networks enables a high quality of service by utilizing the maximum density of active sensors in air networks.	Future information exchange systems could benefit from the optimized active density by maximizing the quality of service for AS.
[24]	Research	2018	Decentralized data transfer IoT Networks	Blockchain implementation opportunities and challenges are discussed, and a use case for integrating blockchain into an IoT framework for protecting sensor data.	Further investigation of implementation and results
[23]	Research	2018	Decentralized Data Storage	Briefly discuss the use of P2P networks to create data storage.	Several technical problems need to be solved regarding private data.
[9]	Review	2018	Decentralized Storage Network with Smart Contract	Propose a novel architecture that utilizes the latest cryptographic primitives and blockchain technology to structure a Decentralized Storage Network.	Security loopholes challenges.
[5]	Research	2017	Decentralized storage	Authors propose a decentralized content placement system that is capable of storing contents independently at each network node	With respect to the lower bound derived, the proposed delivery scheme can be significantly more effective
[15]	Survey	2017	decentralized oracle network	A brief survey of witnet	Witnet protocol can be incentivized, auditable, and verifiable DON construction by implementing state-of-the-art security protocols.
[22]	Research	2017	Decentralized File Storage	Developed a design that involves a distributed storage system in conjunction with a blockchain-based payment system that preserves privacy while providing incentives to participate	The authors did not achieve a trade-off between privacy and security
[7]	Research	2017	Encrypted Decentralized Storage	Examine the proposed architecture's security and performance	An advance architecture is needed for security and performance analysis.
[21]	Survey	2017	Decentralized Storage Network	The working mechanism of file coin	Security challenges and data transfer speed can be discussed further
[6]	Review	2010	Distributed Storage in WSN	Develop decentralized Fountain codes-based algorithms to store data on wireless sensor network	Security and latency challenges

nodes to avoid collapsing if one of the nodes fails. PingER (Ping End-to-End Reporting) is an end-to-end reporting tool proposed by the authors of [9]. Distributed Hash Tables (DHT) store actual files off-chain, while a private blockchain stores metadata about each file.

A. LITERATURE SURVEY

In order to measure Internet performance worldwide, this system removes the centralized party. Search issues in storage blockchains can be overcome with a keyword search service [9].

The below figure 3 is the depiction of the summary of work carried out.

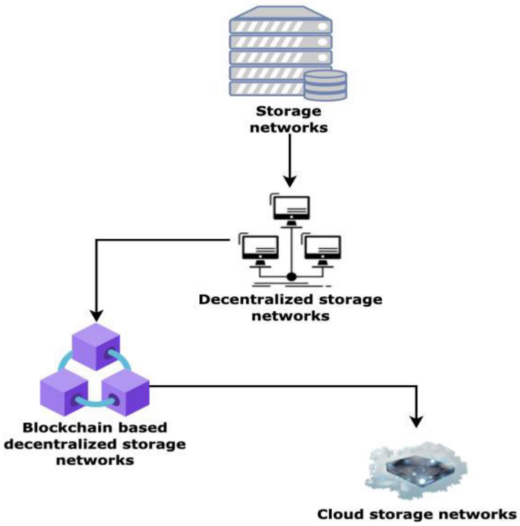


FIGURE 3. **Summary of our findings.**

Data will be encrypted before it is sent over the system's network, and the encrypted data will then be sent to a node (storage provider) to be stored. Nodes grant permissions to each other despite keywords being stored on the blockchain. Data owners and permissioned nodes can search the blockchain as a result. It has been proposed to implement a system for preventing data fraud [10]. There should be meta-data about how the data was acquired, the owner of the data, and how it was transformed; known as Data Provenance, this package tracks the provenance of data. As long as most participants are trustworthy, malicious modifications to data will be impossible [11]. Attribute-based encryption (ABE) is one solution that has been proposed to deal with the privacy problems posed by traditional cloud storage systems. Consequently, traditional cloud storage systems are susceptible to single points of failure. According to [2], blockchain technology provides a single point of failure for decentralized storage. ABE technology, Ethereum blockchains, and interplanetary file systems enable this model to achieve decentralized storage. A keyword search feature is also available on this platform to allow the owner of encrypted data to specify who should have access to the data. A private blockchain, BlockHouse, has been created to convert digital storage into a private blockchain. Blockchain-based storage networks use private blockchains to monetize unused hardware space. The availability and redundancy of data are checked at fixed intervals. Logging, payment, and storage security are all handled by dual intelligent contracts in this network. Consensus is achieved in this project using the PoR algorithm. Rather than storing critical data in the cloud, small and medium enterprises can keep it on their network. According to a study conducted in [1], data distribution systems in organizations were examined. There is a concern that these systems could create a disaster due to the need for data extraction. A decentralized data storage solution was developed using blockchains and artificial intelligence. Blockchain is combined with artificial intelligence for understanding, creating, and retrieving knowledge. With blockchain, you can protect your data and save money at the same time. Every day, the Internet of Things (IoT) grows, as well as the amount of data it generates. Third-party storage spaces store a large amount of essential data, which poses trust issues. To solve this problem, [12] proposes implementing blockchain-based multi-center storage systems, encryption, consensus algorithms, and smart contracts. Artificial intelligence (AI) refers to objects that comprehend their environments and make decisions that increase their chances of achieving their predefined goals. A database helps AI systems make better decisions. The authors have proposed a blockchain for artificial intelligence (AI) [2]. With the blockchain, data can be maintained and kept safe from manipulation and tampering by providing decentralized storage space. This enables proper decisions to be made. Above table 1 portrays a brief survey of research in this domain.

B. CLOUD STORAGE

The use of cloud storage has become a standard across industries and corporate companies, as cloud storage HAS several advantages for enterprises when it is implemented. Similar to how data is generally handled, a cloud's data is basically kept on hard drives [25]. Instead of being stored on individual devices, cloud data is stored on servers owned by large companies. The user can access this data through the internet. Since there is an increasing amount of online digital content, adding storage to the existing infrastructure is necessary to accommodate the need for storage. To accommodate this, expensive servers will have to be purchased, which are hard to maintain and require costly configuration. It is also costly to migrate data from one server to another in the event of a failure. Data storage is a significant undertaking involving an enormous budget to meet the ever-growing demand [26], [27], [28].

C. BLOCKCHAIN SYSTEMS

Blockchains are public ledgers that record peer-to-peer transactions. The peer-to-peer architecture enables networks to scale and operate independently of a central server, even in a computer network failure and with a remarkably transient node population. Blockchains store all the history of transactions, making them very difficult to alter. The first blocks without parents are called Genesis blocks [29]. Transactions are verified using a mining process that solves a computationally tricky puzzle and finds a unique nonce. Blockchain users must vote on a commerce group to create a new block. Using the block as a database is impossible because it can only store vital information.

D. DECENTRALIZATION OF STORAGE

Blockchain has been used in other areas, but recent developments in decentralized storage networks have also become visible. There have been many attempts in the industry to build a decentralized storage network by integrating concepts of blockchain, such as storj.io and filecoin.io. Filecoin, for example, aims to use a novel concept known as Proof-of-Spacetime to create blockchain data storage done by miners. This 'Proof of Spacetime' replaces the conventional 'Proof of Work' used in the blockchain system [30]. New blocks can be mined quickly without wasting time on computations. Instead, by storing information in the network, they extract blocks rapidly. Transactions between clients and providers are conducted with native tokens.

An incentive layer can be added by building an incentive layer on top of the blockchain and using native tokens. A smart contract can also be used to store information about storage capacity and agreements between customers and providers [31].

E. WHY DECENTRALIZED STORAGE DATA?

Because cloud storage is easy to use, ordinary users and large businesses have moved their data to centralized servers. As a result of economies of scale, large data centers have emerged, dominated by tech giants like Amazon, Microsoft, IBM, and Google [32], [33]. Even though competition between corporations ensures that users have a variety of service providers to choose from, the nature of the services is often viewed as a potential source of censorship or misuse of private data. Additionally, experts report a 71% increase in valid data breaches between last year and 2020 because cloud storage is moving to the cloud. Figure 4 shows the stats regarding security breaches in cloud storage [34].

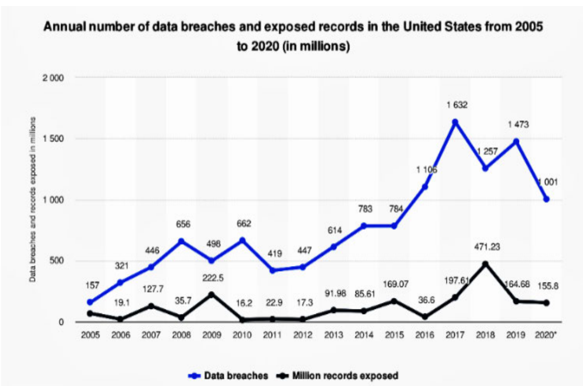


FIGURE 4. **Security breaches in cloud over the years.**

Several ways are being explored to disrupt the existing cloud market with decentralized storage networks. To start with, these networks are most likely to operate based on free markets, with open participation. In this way, it is possible for anyone to participate in the network, and rather than relying on a single point of failure, data is replicated across multiple nodes. Furthermore, public-key cryptography is a natural accompanying feature of blockchain integration [35]. A host usually encrypts data before it is stored, so it can only be decrypted by the rightful owner and any parties he or she has agreed to share it with. The process makes these services more resistant to censorship and manipulation, as well as rendering any data compromised in a breach useless to an attacker [36].

1) INCREASED SPEED

As opposed to centralized storage, peer-to-peer systems rely on peer-to-peer technology [37]. Data transmission does not occur through the central server during peak traffic times. Multiple copies of data are stored at different locations, so downloads are faster.

2) LOAD BALANCING

Blockchain-based decentralized storage systems follow the principle of load balancing. Data can be cached locally by hosts to avoid repeated access to the server [38]. The server is relieved of the burden, and the network traffic is also eased. In addition to allocating and optimizing data, the server can reduce bottlenecks in the central system.

3) FAIR MARKET PRICE

Decentralized storage systems become a perfect competition when there are millions of nodes. Individual nodes cannot charge higher prices. Prices are, therefore, equal across all nodes. This market ensures that only high-quality nodes survive and compete [39].

4) INCREASED SECURITY AND PRIVACY

The high level of security provided by decentralized data storage systems is their most significant advantage [40]. Shared data is broken down into smaller chunks using hashes or public-private keys to encrypt copies of the original data and share copies of the original data with each other. The entire process is secure by securing the data from bad actors [41]. Further, no owner information exists in any stored data, which is not the case with centralized systems.

F. ADVANTAGES OF DECENTRALIZED STORAGE DATA

As an alternative to centralized storage, peer-to-peer storage is emerging as a disruptive force. Here are a few advantages a decentralized storage system provides.

1) HIGH RELIABILITY

Multiple hosts are used in the decentralized network to distribute and store data. Redundant copies of the data are stored (eliminating a single point of failure). Backup copies will be available in case of a hardware failure or loss. A unique hash value is also assigned to each chunk of shared data [42]. By adding this extra layer of protection, data becomes more secure.

2) LOW COSTS

A decentralized data storage system significantly reduces both hardware and storage costs. In an environment of decentralization, machine performance requirements are reduced, which decreases the need for expensive investments in high-performance hardware and software. Moreover, there is a potential for millions of nodes to store data in the decentralized network. Therefore, the available storage space has increased significantly [43]. This system continuously utilizes all the idle storage space, reducing waste and avoiding the need to invest in new storage. Compared to centralized cloud storage, the overall storage cost is significantly lower [44]. A quick comparison of centralized and decentralized storage networks is presented below in Table 2.

G. P2P NETWORKS

P2P nodes can serve as both clients and servers. File-sharing P2P networks, also called decentralized public storages, are intended for sharing files between all network users [45]. A particular network provides tools and methods that allow users to search for desired files and download them from other computers (in this scenario, the files are open for everyone to access) by employing its search tools. Users gain access to their files within a P2P network and the ability to search for and download files after installing a client program on their computer. The parts of a file that have been downloaded instantly become sources for other users in many networks when they download a file from several sources simultaneously [46]. BitTorrent is a classic example, which ensures high bandwidth on P2P networks. Commonly, P2P networks connect computers from different administrative domains. As P2P networks are dynamic, participants can frequently join or leave them. A virtual overlay network on top of the Internet is formed by P2P nodes that coincide with Internet nodes and store information about several other nodes. Physical links in the core network correspond to each link in the overlay P2P network. In a P2P storage system, data must be efficiently searched for and fault-tolerantly stored, and queries and responses must be routed accordingly [47]. Several types of infrastructures and algorithms are developed to meet these requirements. Based on distribution control techniques, data search techniques, and overlay network topologies, P2P networks can be classified [48].

Although P2P networks are commonly assumed to be fully decentralized, they are not always decentralized; some may be more centralized than others. A single central server in centralized P2P network stores the central resource register and other information about the network. The central registry server allows network users to locate desired files by querying its address. A single point of failure exists in such P2P networks because they are poorly scaled. Depending on their characteristics, these systems can be categorized as fully decentralized or hybrid. Network nodes play a different role in each. There are no differences among nodes in a fully decentralized system (for example, Gnutella and Chord) [49]. Certain nodes in hybrid systems assist other ordinary peers in processing search queries. These nodes are called dominating nodes or super peers. Computing power, stability, and Internet connection quality are often heterogeneous among peers in P2P networks. A fully decentralized system can utilize the heterogeneity of a hybrid system, but not a fully decentralized system. The super peers are assigned the task of indexing dynamically and caching the files stored in small parts of the overlay network. They act as proxy servers, indexing the

TABLE 2. Comparison of centralized and decentralized storage.

Attributes	Decentralized Storage	Cloud storage (Centralized)
Main use case	Storing files at hypercompetitive prove	Storing files using a familiar widely-supported service
Pricing	Determined by a hyper-competitive open marketing	Set by corporate pricing departments
Centralization	Large numbers of storage providers	A few big companies
Reliability	Independently checked by the network and publicly verifiable	Companies self-support their own stats
API	The application can access all storage providers using the file coin protocol	Applications must implement a different API for each storage provider
Open Source	YES	NO
Fault handling	If a file is lost, the user is refunded automatically by the network	Companies can offer users credit if files are lost or unavailable
Scalability	Complicated	High
Physical location	Miners located anywhere in the world	Limited to were provider's data centers are located
Privacy	High	Low
Cost	Low	High
Retrieval	The competitive market for retrieving files	Typically, more expensive than storing files to lock users in
Ability to choose hardware type	YES	NO
Payment method	Cryptocurrency	Fiat money
Support	If something goes wrong, the file coin protocol determines what happens without human intervention	If something goes wrong, users contact the support help desk to seek a resolution
Data processing	No	YES
Becoming a storage provider	Low barrier to entry for storage providers (Hard drive, internet connection)	High barrier to entry for storage providers (legal agreements, marketing, support staff

files provided by the ordinary nodes associated with them and performing searches on their behalf. Because of this, super peers receive all queries first [50]. It is important to choose dominating nodes carefully to avoid bottlenecks and single points of failure. The decentralized P2P networks are divided into two categories based on their structure: structured P2P networks and unstructured P2P networks. Most of the time, this is done automatically. The architecture and data allocation of structured P2P networks are precisely defined. A distributed hash table (DHT) facilitates the identification of content by efficiently directing queries to a node that contains it by ensuring correspondence between data (e.g., a file id) and its location (e.g., a node address). These networks make it possible for systems to be highly scalable. Although they provide efficient message routing in the medium with a variable number of nodes, their disadvantage is the complex management of the network structure. Network topologies and data storage locations in P2P networks are unstructured, and there are no rules to govern them [51]. Two simple search mechanisms use query flooding and route indexing to find desired data by flooding queries in a depth-first or breadth-first manner. Availability, reliability, and scalability are all issues associated with unstructured networks, which are much harder to deal with [52]. Unstructured systems, on the other hand, are better suited to networks with variable nodes. The overlay topology and the data search/allocation have a probabilistic nature based on certain assumptions. Both properties can be combined to achieve different data distribution/retrieval properties. Overlays are defined probabilistically, while data locations are precisely determined. A weakly structured network resides somewhere between a structured and unstructured network [53]. P2P systems can also be classified based on other characteristics. Hierarchical and non-hierarchical overlay networks can, for instance, be classified according to whether they have a hierarchy. In most fully decentralized systems, overlay networks are flat, so they are nonhierarchical.

Hierarchical systems comprise all hybrid systems and some fully decentralized systems. Load balancing and stability are inherent to non-hierarchical systems [54]. The hierarchical structure of a network improves scalability, routing, and performance by utilizing the heterogeneity of nodes. Decentralized P2P networks can also be classified based on different characteristics. The figure shows an example of a decentralized P2P network classified by different characteristics. A taxonomy of P2P network Classification is presented in figure 5.

Blockchain technology is being applied in various domains; several researchers presented brief research on multiple aspects of decentralized storage, such as technology used for decentralization, problems, and their solution in decentralized storage. Some dealt with future elements and challenges. The technology has the potential to revolutionize storage networks by providing autonomous financial settlement, audit, and reconciliation mechanisms with greater transparency by preventing fraud. The authors present various

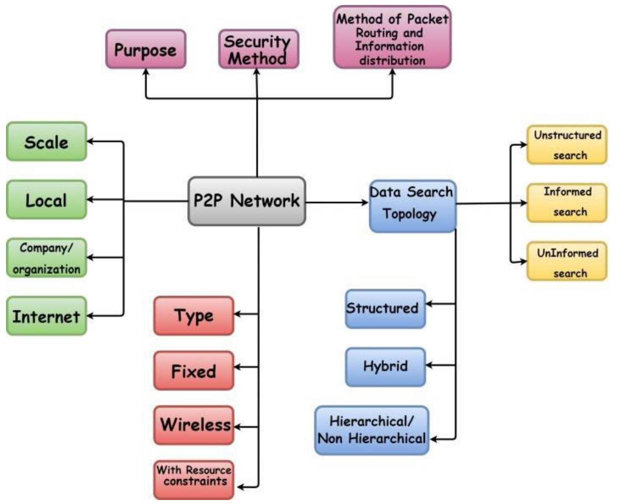


FIGURE 5. **P2P network classification.**

models with public and private block chains and highlight potential attacks along with their solutions. In most surveys and reviews, we observed a vertical-specific approach and a lack of comprehensiveness—all sections of this work present vertical-specific coverage over a wide range of studies. Below in table 3 a comprehensive overview of various papers on block chains in storage networks.

IV. BLOCKCHAIN-BASED DECENTRALLIZED STORAGE NEWORKS

There are various blockchain-based decentralized storage networks available in mainstream market for storage rental services.

A few DSN storage giants are discussed as follows.

A. STORJ, A DECENTRALIZEDSTORAGE NETWORK

1) WHO CREATED STORJ

Shawn Wilkinson and John Quinn founded Storj Labs, the company behind the Storj platform, in 2014. In September 2019, Storj V3 was launched as the newest version. Since its founding, Storj Labs has been funded in three rounds. In 2017, Storj migrated from Bitcoin to Ethereum after launching on Bitcoin. In 2014, Storj Labs raised 910 bitcoins (worth approximately $460,000 at the time) in a public crowd sale. A token sale in 2017 raised $30 million after Storj raised $3 million in seed funding [81].

2) HOW DO STORJ WORKS?

Storj is an open-source cloud storage network based on peer-to-peer and remote technologies. Storj is a hybrid network designed with both elements of centralized and decentralized architectures. The web is viewed as decentralized from the storage perspective since the content is segmented and distributed across many peers. Storj relies on centralized servers for communication control [82]. A centralized server manages user authentication and facilitates exchanges between peer storage nodes in addition to facilitating encrypted file segment storage on peer storage nodes. Several different

TABLE 3. Survey of block chain in storage systems.

References	Technology	Solutions	Future Aspects	Challenges Faced	Security, privacy	Traceability	Secure storage	Public block chain	Private blockchain	Fully decentralized	Possible attacks
[33]	×	×	✓	×	✓	✓	×	✓	×	×	×
[55]	✓	×	✓	✓	✓	✓	✓	✓	×	✓	×
[56]	✓	✓	✓	×	×	✓	✓	✓	✓	✓	×
[15]	✓	✓	×	✓	×	✓	✓	✓	✓	×	×
[57]	✓	✓	×	✓	×	✓	×	×	×	✓	✓
[58]	✓	✓	×	✓	×	✓	✓	×	×	×	×
[55]	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
[59]	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[60]	×	×	✓	✓	✓	×	✓	×	✓	✓	×
[16]	×	×	×	✓	✓	×	✓	✓	×	✓	×
[61]	×	×	×	✓	✓	×	✓	✓	×	✓	×
[62]	×	✓	✓	×	✓	×	✓	✓	✓	✓	×
[63]	✓	✓	✓	×	✓	✓	✓	✓	✓	×	×
[62]	✓	✓	✓	×	×	✓	✓	✓	✓	×	×
[64]	✓	✓	×	✓	✓	×	×	✓	×	×	×
[65]	×	✓	×	×	✓	×	✓	✓	✓	×	×
[66]	×	×	✓	✓	×	✓	✓	✓	×	✓	×
[19]	×	×	✓	×	×	×	×	×	✓	✓	✓
[67]	×	×	✓	×	✓	✓	×	✓	✓	✓	✓
[68]	×	×	✓	✓	✓	✓	×	✓	×	×	✓
[69]	✓	×	✓	×	✓	✓	✓	×	×	✓	×
[70]	✓	✓	✓	×	✓	✓	✓	✓	✓	×	✓
[71]	✓	✓	✓	✓	✓	✓	✓	×	✓	×	×
[72]	✓	✓	✓	✓	✓	×	×	✓	×	✓	✓
[73]	✓	×	✓	✓	✓	✓	×	✓	✓	✓	✓
[74]	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓
[75]	✓	×	×	✓	×	×	×	✓	×	×	×
[17]	✓	×	×	✓	×	×	×	✓	✓	✓	✓
[76]	✓	✓	✓	✓	×	×	×	×	✓	×	×
[77]	✓	✓	✓	✓	✓	×	×	✓	×	✓	×
[78]	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×
[20]	✓	✓	✓	✓	✓	✓	✓	×	×	×	✓
[79]	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
[80]	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×

units make up the Storj network. A bridge, a renter, or a provider are among these. The Storj network rents out space to users [83]. Users upload and download files using Storj's Client application, which allows them to interact with the network. The renter must first interact with the bridge to communicate with the network. A bridge grants the renter permission to send and receive files from Providers after that conversation. That bridge is the network's central element.

The bridge interacted with every element in the network and delegated all communication except for the files transmitted between renters and providers. It is the gateway through which the network is accessible to both renters and providers. By observing all connected providers and renters, the bridge also periodically checks the status of the network [84]. A provider is a network user that offers storage. To participate in the network, they must first request permission from the bridge. A bridge must approve for them to join the network. Renters can engage providers for drive space once providers join, allowing them to establish storage contracts. Several steps involve uploading a file to a peer-to-peer cloud storage provider. An agreement must be established between the renter and the provider before a file can be handled. Following the completion of the necessary contracts, the files are queued for upload after being stored on the bridge [85]. As part of the process, the renter encrypts the file and segments it into shards. Upon creation, the shards are distributed among the providers according to the contract [86]. As a backup mechanism, redundant copies of the shards are created and distributed in case a provider loses, destroys a share, or goes out of service when the renter needs to access shards. When a renter wants to download a file, they contact a bridge to request it from a provider. First, the bridge determines if it can reassemble the file based on the shards available so that the renter can download it. If a file can be rebuilt, the bridge notifies the provider to begin sending the shards to the renter. Once the renter has all the shards necessary for restoring the file, the shards must be combined into one file and decrypted. Now that the file has been retrieved and is stored on the renter's computer, the bridge can audit the transaction [83].

3) STORJ NETWORK COMPONENTS

Three main components contribute to powering the Storj network are:

a: STORAGE NODES

Providing users with the option to rent out excess space on their hard drives and store and recover data for a fee.

b: UPLINKS

Upload files to a network by running on the client's machine. Also, uplinks coordinate data storage and retrieval between peers.

c: SATELLITES

Ensure that traffic between storage nodes and uplinks is coordinated. The satellites are responsible for storing metadata, supervising storage nodes, and distributing payments. The satellites have a user account for each user.

d: SEGMENTS AND STRIPS

Storj files go through a segmentation process once a user's satellite permits to store data on the network. This process involves compressing, encrypting, and then shredding files, i.e., dividing them into segments and stripes. Those stripes are then distributed over the internet as copies of the original files. Users must provide the same password used to compress and encrypt their files to be able to decrypt them and retrieve them. Segments that are small enough are typically stored in a satellite instead of a storage node. The concept of redundancy is what Storj uses to account for the potential loss of a stripe when a node shuts down [87]. The technique duplicates all stripes a certain number of times, preventing any small number of nodes from tampering with or censoring them. Figure5 shows the connectivity of Satellites for storage node operators.

e: FILE VERIFICATION

An audit of each file is performed by Storj every hour. The provider nodes must prove they have the shards they've been sent before they can get paid. Storage sends a request to provider nodes; if a provider node has modified or deleted the encrypted shard, it can't respond. Provider nodes can respond to requests correctly if they currently hold the file. A micropayment is made to the storage provider node for storing and maintaining the file. This incentivizes provider nodes to store the files and remain active on the network. It is being considered whether to implement a reputation system for provider nodes [88]. The system would determine which nodes offer high bandwidth and operate honestly.

f: BRIDGE

The bridge is one of Storj's latest initiatives. A tenant's private encryption keys were previously stored on their local computer [83]. Using the Bridge server, encryption keys can be stored without centralized control. Multi-device access is possible because keys are safely stored. Providing users with access to files is the next step. Since files are already stored in the cloud, decentralized file sharing requires only a simple verification of identity and permission [89].

g: TOKEN

Payment is made with the Storj token. Storage providers get paid by tenants to provide storage space and bandwidth to the network. Open-source Storj is payment agnostic, contrary to Storj Labs, whose implementation exclusively uses tokens. The assumption is STORJ, but other coins can also be used, such as BTC or ETH [37].

-Distributed in ICO: Up to 25% (June 2017)
-Emission rate: No new coins created.
-Consensus: Proof of Work
-Token supply: 500 million
-Blockchain: Ethereum

Table 4 portrays the current stats of the storj network around the globe.

4) ADVANTAGES OF STORJ

a: SECURITY

AES-256 encryption is used to encrypt the files and their metadata, and the system distributes erasure-encoded pieces of each file to a diverse set of Storage Nodes across the globe. It is simple and secure because the encryption keys are generated automatically [90]. Users can access data only with

TABLE 4. Current stats of the storj network.

Active Nodes	12,751
Free Capacity	6.2 PB
Objects	402 million
Object Pieces	31 million

permission from the owner. As an added layer of security, Storj DCS pushes access management to the edge using macaroon-based API keys. Eighty or more pieces of a file are stored on different nodes. Only 29 parts are needed to retrieve and reconstruct a file [91].

b: PRIVATE

Many attacks involve gaining access to a trove of data, compromising a credential, or breaching a central repository of access controls. This is no longer possible with decentralization. As Storj DCS manages access peer-to-peer, it separates responsibilities for creating bearer tokens and encryption [92]. Separating these concerns allows greater privacy and transparency through decoupling data storage, access management, and use [93].

c: AVAILABILITY

By default, the data stored by the DCS is available worldwide over a global network of storage nodes. Storj DCS stores data on Nodes that are chosen based on reputation and local latency [94]. This set of Nodes is desired to store chunks of your file, ensuring quick access to data. Storj gateway libraries enable applications to take advantage of massive parallelism from both a download and upload perspective directly at the edge [95].

d: PERFORMANCE

Parallel, peer-to-peer file transfers using Storj DCS are faster, more reliable, and deliver 119s of durability and uptime. Data is accessible on demand from anywhere worldwide thanks to multi-threading concurrent downloads and uploads of files. With centralized storage services, data is recovered slower than the fastest data restore. More than 13,000 nodes around the world ensure low latency and high throughput, regardless of where data is being downloaded from [96].

e: OPEN SOURCE

The codebase of Storj is open source. As part of the open-source project, developers can contribute to the development of decentralized architecture, which enhances the security and privacy of users through transparency [97].

5) POTENTIAL VULNERABILITIES OF STORJ

-Due to the volatile nature of networks, clients must implement data redundancy schemes proactively.

-Clients are more likely to lose data due to inconsistencies in storage provider nodes [97].

-The problem with storage provider node storage networks isn't that they are not economically scalable; rising electricity costs will eventually make a storage node unprofitable [98]. No one can control the availability of a storage node so that it can be turned off or broken at any time. Consistency in networks is what this is all about.

-HTTP is used to transfer data. Shards can be uploaded or downloaded from endpoints exposed by storage providers. Exposing their IP addresses allows storage provider nodes to be hacked [99]. The bridge is designed only to store metadata and is thus a central point of failure for Storj [100]. Decentralized storage models work off the premise that not everyone will be able to utilize the storage that their devices have on them. This leads to individuals being incentivized to rent out their unused hard disk space to users in exchange for payment. Decentralized storage has several benefits, including the security guarantees provided by blockchain technology and the possibility of safer storage alternatives. Several nodes in the network keep copies of the information, so there are no single points of failure in the network. Moreover, due to the distributed architecture of DCS networks, it is theoretically impossible to steal user data or restrict access to them because the DCS network is distributed. Various decentralized storage networks are available in the market for sellers and renters. A quick comparison through a pie chart is presented in figure 6 below.

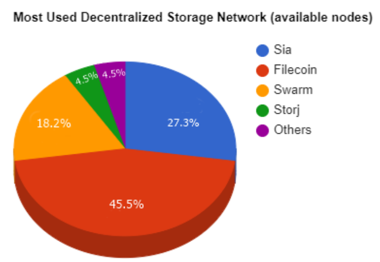


FIGURE 6. Most used decentralized storage network.

Table 5 portrays a quick comparison between different decentralized and cloud storage networks.

B. FILECOIN IS A DECENTRALIZED STORAGE

The FileCoin network is a decentralized storage network. This system uses IPFS as its backend. The Interplanetary File System (IPFS) is a distributed peer-to-peer file system that eliminates single points of failure by connecting all computing devices in a network [101]. Data can be stored on third-party storage space offered by FileCoin, whose trustworthiness clients can't verify. Like any other decentralized storage system, these networks must be protected throughout their lives [102].

Two methods are proposed by File Coin to meet this demand.

-Proof of space-time: this method ensures clients that their data will be kept for a specific period.

TABLE 5. Comparison among storage systems.

Attributes	Amazon (Cloud)	File Coin (IPFS)	Sia	Storj	Swarm
Network	Centralized	Decentralized	Decentralized	Decentralized	Decentralized
Privacy	Low	High	High	Very High	High
Online time	Occasionally offline	All time online	All time online	All time online	All time online
Security	High	Very High	Very High	Very High	Very High
Mining time	×	20min	30 min	30 min	–
Public chain	×	YES	YES	NO	YES
Miner	×	NO	NO	NO	NO
Cross-chain	×	YES	NO	NO	NO
Smart contract	×	NO	YES	NO	YES
Peer-to-peer market	×	NO	NO	YES	NO
File system	×	YES	NO	YES	NO
Data sharding	YES	YES	YES	Automatic Sharding	YES
Ensure Correcting	YES	YES	YES	YES	YES
Upload speed	–	Smart adjustable	1M/s	0.3M/s	No Data
Dapps	×	YES	NO	NO	NO

-Proof of replication: proof-of-replication can demonstrate that data is protected in its physical location and that none of the network nodes have duplicate files on their hardware.

1) HOW FILE COIN WORKS

Users and storage providers play vital roles in the File coin network, which is a peer-to-peer network [103]. Mines in the File coin network have computers with internet connections and space that they can hire. Miners are the storage providers contributing storage to the network in exchange for FILs. In the meantime, the users seek to purchase storage from the storage providers implementing the Filecoin protocol [104]. At first, glance, keeping valuable information on someone else's computer may seem risky. File coin breaks down data before storing it to ensure that hackers cannot access data stored within its network. As a result, a malicious actor would only see meaningless data bits if they attempted to access a file on the Filecoin network. The agreement between a storage provider and a user is called a contract. Two types of Filecoin deals merit mention: storage deals and retrieval deals. According to their names, storage deals occur when the miner receives data from a client to store, and retrieval deals occur when the miner withdraws data from the network. After a storage contract is signed, miners must continuously prove that they are serving clients well by storing their data [105]. Keeping third parties out of the network is achieved through File coin's consensus mechanisms. Filecoin verifies storage data through ''proof of replication'' (PoRep) and ''proof of space-time'' (PoST) to prove to the network that the storage is occurring as specified in the deal between the client and the miner [8]. Data is encoded in PoRep by a storage provider, designed to happen slowly. It is then the storage provider's responsibility to prove that the encoding of the data is unique. Due to the gradual nature of the encoding sequence, if the storage provider responds quickly, it means that the data has been encoded and is being stored safely. If the storage provider does not respond immediately, they have generated a new encoding and are not acting in good faith [106]. Through PoSt, miners prove the data is stored continuously in storage once a deal has been made between a storage provider and a user. Depending on the amount of data, random miners prove the data is still available [107].

2) FILE COIN STATA IN 2022

-Total storage capacity of 12 EIB

-3,362 Filecoin storage providers

-More than 230 organizations have joined the network

-Approximately 465 new projects have been added to the ecosystem

-7500+ contributors on GitHub projects

-A hackathon attracts 10,000+ developers.

3) FILE COIN (A DSN CONSTRUCTION)

Filecoin DSN aims to be an auditable, publicly verifiable, and incentive-driven decentralized storage system. In exchange for payment, clients pay a network of miners for data storage and retrieval. The network only pays miners if it confirms that the service was provided correctly [108].

a: PARTICIPANTS

The system allows users to be either a Client, Storage Miners, or a Retrieval Miner.

b: CLIENTS

Clients are charged for storing data and retrieving data from the DSN.

c: STORAGE MINERS

Storage miners provide network storage. For participating in Filecoin, storage miners offer their hard drives, and servers put requests [109]. Users who wish to become Storage Miners must deposit collateral proportionate to their storage space. Storage miners commit to storing a client's data for a specified amount of time when they submit put requests. To demonstrate the validity of the data, storage miners create Proofs-of-Spacetime, which they submit to the blockchain. Invalid or missing proof penalizes Storage Miners and causes them to forfeit the collateral. Additionally, storage miners can also mine new blocks. They receive mining rewards and transaction fees for creating a new block [110].

d: RETRIEVAL MINERS

The Network's retrieval miners provide data retrieval services. Filecoin retrieval miners gather data from getting requests made by users. These miners do not have to pledge, commit, or provide evidence of storing data like Storage Miners. Storage miners typically play a role in retrieval mining as well. The retrieval miner can purchase pieces directly from clients or through the retrieval market [111].

4) ADVANTAGES OF FILE COIN

a: VERIFIABLE STORAGE

A built-in process in Filecoin verifies that files are stored correctly and validates their history. During every 24-hour period, storage providers must prove that their files are being maintained [112]. This history can be scanned efficiently by clients if they were offline at the time, to ensure that their files are correctly stored. A knowledgeable observer will notice whether any storage provider has been faulty or unavailable in the past if they check their track record [113].

b: OPEN MARKET

A Filecoin exchange is an open marketplace for negotiating files storage and retrieval deals. You are not required to have permission to join Filecoin's network. You simply need an internet connection and spare disk space to run a miner. A thriving ecosystem of independent storage providers is enabled by Filecoin's lowering of entry barriers [23].

c: OPEN-SOURCE CODE

A client and a storage provider can both run the open-source code [114]. Software for managing storage infrastructure does not need to be developed by storage providers. The code of Filecoin has been improved in a way that benefits everyone [18].

d: SINGLE PROTOCOL

Any miner that implements the Filecoin protocol will be able to store data for applications that implement the protocol. There is no need to implement different APIs for different providers. A third party application supporting multiple providers is not limited to features that all the providers support on a lowest common denominator basis [111].

e: CONTENT DISTRIBUTION NETWORK

These computers are connected to a good network, which makes them ideal for retrieval mining. As retrieval miners distribute popular files to nearby users, they are rewarded for smoothing network traffic and accelerating file downloads [115].

C. SIA (A DECENTRALIZED STORAGE NETWORK)

The idea for Sia came from David Vorick and Luke Champine at HackMIT in 2013. A decentralized cloud storage platform built on blockchain technology called Sia was developed by the nebulous team based in the United States and European Union. Sia increases data storage reliability and affordability by leveraging unutilized hard drive capacity globally. Powered by a utility token, Sia has its own blockchain. It is important to ensure high availability by storing data worldwide to eliminate any single point of failure [116].

1) SKYNET

On top of Sia's cloud storage network, Skynet is a decentralized platform for sharing and delivering files and content [53] [117]. Skynet enhances Sia with file sharing, data publishing, and the infrastructure required to allow apps to serve content in a decentralized way. Skynet can host all types of data. Files can be uploaded through a Skynet Web portal or Sia node. When a file has been uploaded, it generates a 46-byte link known as a Skylink. Anyone can use that link to download Skynet data, whether they are Sia users or not. The original uploader does not have to stay online to keep the file available. Sia does all pinning in real-time, ensuring excellent uptime and high speeds. Decentralized applications benefit from this since they can run confidently, knowing that their storage layer is just as decentralized as their applications. Skynet can store and distribute data in a low-cost, low-hassle, high-speed manner. Traditional infrastructure costs 10x more than cloud storage, while bandwidth is 100x cheaper, all without sacrificing performance or reliability [118].

2) HOW SIA WORKS

Following are a few important SIA terms explained.

a: NODE

Installation or instance of Sia.

b: RENTER

An individual who uploads files to a network.

c: HOST

An individual who lends their storage space to others to upload files.

d: CONTRACTS

In contracts between a host and a tenant, the amount, length, and prices of data storage are specified. Blockchain and software automate the process of tracking and completing these tasks.

e: SIA COINS

The crypto currency that powers Sia.

f: SIA FUNDS

The Siacoin token is a secondary token that grants its holder Sia coins for completing contracts. The Sia platform splits files, encrypts them, and sends them globally. Both hosts and renters upload files throughout the entire process. Whenever a file is uploaded, it is copied multiple times so the owner can access it at any time [119]. Since hosts only receive parts of encrypted files, they can never access them. User ranters upload files to Sia, while user hosts make their space available for other users to store data for a certain period and a certain amount of money.

3) ADVANTAGES OF SIA

a: COMPLETELY PRIVATE

Sia uses a decentralized network to encrypt and distribute files. Private encryption keys are yours to control, and data is yours to own [120]. In contrast to traditional cloud storage, your files can't be accessed or controlled by a third party or outside the company.

b: FAR MORE AFFORDABLE

Sia's decentralized storage costs 90% less than incumbent cloud storage providers. A 1TB file on Sia costs about $1-2 per month, while a 1TB file on Amazon S3 costs $23 [121].

c: HIGHLY REDUNDANT

The Sia platform distributes and stores redundant file segments across nodes in multiple locations worldwide, eliminating a single point of failure and guaranteeing uptime that rivals traditional cloud providers [122].

d: OPEN SOURCE

An active community of developers builds innovative applications using Sia APIs, and its software is entirely open-source [123].

D. PRICE EVALUATION AND COMPARISION

Various DNS providers provide storage facilities at different prices in terms of bandwidth. The figure 7 shows the comparison of different decentralized storage networks:

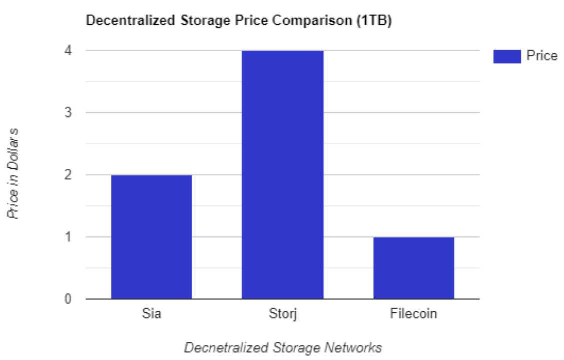


FIGURE 7. Price comparison of different DSNs.

V. POSSIBLE ATTACKS ON DECENTRALIZED STORAGE NETWORKS AND SOLUTIONS

Distributed systems are vulnerable to a variety of attacks [124]. Some attacks can affect any distributed system. These attacks tend to be storage-specific and can affect any distributed storage system.

A. SPARTACUS

On Kademlia, it is possible to suffer a Spartacus attack or identity theft [125]. Any node can assume the identity of another by copying the Node ID and receiving some fraction of the messages intended for that node. Nodes and data can be targeted using this method [126]. All messages must be signed, and Node IDs are implemented as ECDSA public key hashes. This would prevent Spartacus attackers from signing messages or participating in the system if they attempted to attack it [127].

B. SYBIL

An attack called Sybil involves setting up large numbers of nodes to disrupt a network by dropping messages or stealing them. As Sybil attacks rely on redundant messages and a concrete distance metric, they are somewhat difficult to conduct on Kademlia. Most messages are sent to at least three neighbors of each node in the network, selected according to their Node IDs. Sybil attacks successfully isolate only 12.5% of honest nodes when they control 50% of the network [128]. The network will still function even though its reliability and performance will degrade until a large portion is made up of colluding Sybil nodes.

C. GOOGLE

This hypothetical attack is carried out by a nation-state with high resources and is somewhat like the Sybil attack. As a result of the difficulty of predicting Google's actions, it can be challenging to defend against a Google attack. Google attacks can only be protected by creating a network with resources equal to those of the attackers. Aiming for the network at that level would require a lot of resources that would not be sustainable [129].

D. HONEST GEPPETTO

A variant of Google's attack, Honest Geppetto, targets storage devices [130]. In the network, the attacker operates an enormous number of puppet nodes, accumulating trust and contracts over time [131]. Once he reaches a certain threshold, he drops each node from the network or pulls the strings on each puppet to execute a hostage attack on the data. A large network can render an attack ineffective, just as it did with the previous attack [49]. This can be partially addressed by relatedness analysis of nodes until then. When downtime, latency, and other attributes are applied to Bayesian inference, data owners should distribute shards across as many unrelated nodes as possible [132].

E. ECLIPSE

An eclipse attack isolates a node or set of nodes in a network graph by ensuring that all outbound connections reach malicious nodes [23]. The Eclipse attack can trick malicious nodes into functioning normally, eclipsing only particular important messages. Overtaking the target node requires generating key pairs until the attacker finds three keys whose hashes are closer to the target's ID than the node's nearest non-malicious neighbor and protecting this position against new nodes with closer IDs. The network has nodes, making this a proof-of-work problem with proportionally increasing difficulty as nodes are added. To defend against eclipse attacks, increase the number of nodes in the network [133].

F. HOSTAGE BYTES

Storage-specific attacks like the hostage byte attack are used to extort additional payments from data owners through the refusal of malicious storage providers to transfer shards or portions of shards [2]. By storing shards redundantly across several nodes, data owners can protect themselves from hostage byte attacks [134]. The malicious storage provider node cannot determine the last byte if the client keeps its erasure encoding secret. Most practical applications of this attack are addressed by redundant storage. However, redundant storage is not a complete solution. Multiple malicious nodes have to cooperate to defeat redundancy, which is very hard to carry out in practice [135].

G. CHEATING OWNER

The data owner may refuse to verify that the audit is true and thereby avoid paying a data storage provider for the data storage. Data owners' shards may be dropped by the storage provider node [6]. As a result of this attack, any future distributed reputation system will have difficulty verifying its claims. Currently, there are no publicly verifiable proofs of storage and no independently verifiable process to confirm whether a privately verifiable audit was sent or responded to as planned [136]. Any reputation system still faces the problem of cheating clients [137].

VI. LIMITATIONS OF DECENTRALIZED STORAGE NETWORKS

Undoubtedly, decentralized storage systems have their downsides, regardless of their potential. The technology is in its infancy, so researchers are trying to find solutions to its challenges [138]. The following are a few challenges associated with decentralized data storage systems based on blockchains:

A. LACK OF TRUST

Using peer-to-peer technology, data is stored DE centrally in a way that circumvents centralized regulations [139]. The decentralized network may be hard for businesses and consumers to trust because of the lack of accountability in cases of lost data or lost transactions. The developers of the decentralized network are working on adding the highest levels of security because of this lack of trust [140]. New technology may take time to gain the confidence of businesses.

B. COMPLICATIONS IN DEVELOPMENT

The consensus mechanism gets complicated when developing a blockchain-based decentralized storage network. Proof-of-Storage (PoS) is based on a consensus mechanism [105]. By verifying the integrity of remote files, PoS ensures their authenticity. To explain this, each node in the system must demonstrate that the data they submit qualifies them to add new records [141]. Users would otherwise believe that the blockchain network had faulty processes due to the consensus mechanism. Although the consensus mechanism is relatively complex, as any developer will tell you, it is worth paying attention [142]. The process will be much easier if you hire a blockchain development company with an extensive portfolio of completed projects.

C. MITIGATION-RELATED CONCERNS

In its infancy, decentralized storage technology will remain in this stage for some time. Due to performance issues, businesses and consumers do not immediately adopt decentralized storage systems [102]. Early adopters should seize the opportunity to implement this strategy before it becomes a mainstream technology. Performance-related challenges are already being addressed by developers [143].

D. SECURITY CONCERNS

The network can, however, be hacked even if it is bulletproof by malicious nodes, launching hub-attacks, disrupting, and potentially destroying the entire system. Blockchain-based decentralized storage systems are currently being developed to prevent these attacks [8], [144].

E. NEED TIME TO GO INTO MAINSTREAM

All the problems associated with centralized storage are undeniably resolved by decentralized storage. There are numerous advantages to decentralized storage over traditional, mainstream storage systems [145]. To be widely adopted, the decentralized system must provide a superior service to the current market. Now, technology is in its infancy. It will remain a niche until it becomes more widely used among businesses [146].

VII. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

As this technology is still in its infancy, numerous improvements are yet to be made. Our discussion in this section covers the issues individuals and organizations face with respect to blockchain-based storage [147].

A. SECURITY

Even though blockchain networks offer greater security than centralized systems, it should be noted that blockchains may not provide complete security. Because decentralized networks are much less likely to encounter security issues than centralized networks, they are less likely to arise, but they are not entirely avoided. Security issues can also occur if data must be edited or shared with a third party because encrypted files have to be decrypted and re-encrypted every time [148]. Furthermore, data is only secure if stored, not sent over a network. Again, some attacks could seriously damage the blockchain itself and its applications. Launching a 51% attack against chains that use the Proof of Work consensus algorithm is possible. Blockchains can be controlled by nodes with high computing power, leading to attacks such as selfish mining and double spending. Having many nodes will prevent these attacks so that no single group can control the blockchain. A selfish node may discover a nonce before others but keep it to themselves and mine until the proofed chain has caught up to them. Following that, they reveal their private chain, and if it is longer than the others offered, they win the prize. This mechanism prevents selfish mining. This method suggests accepting either the latest validated block or the first block received. If two blocks have the same amount of validation, nodes should accept the first block received. Nodes engage in double spending when they spend the same amount of cryptocurrency in multiple transactions. For this problem, the Listening Period technique or waiting for more confirmation has been proposed [148].

B. INSUFICIENT DATA FOR DECISION MAKING

In many companies and organizations, the collected data is regarded as a valuable resource that can be analyzed and processed to aid their decision-making process. Due to the encryption of all data before storage, blockchain-based storage systems cannot accomplish this process. Data can be stored in a blockchain-based storage system such as Block House by companies giving permission to certified agents. In this chain, all the information can be retrieved and analyzed by the agents of a company based on the needs of the company. Moreover, private blockchains with accredited members do not require data encryption. With the use of blockchain, data can be stored in a safe, secure, and trackable manner [149].

C. LACK OF LEGAL RESTRICTIONS

Two parties to smart contracts can't deny or violate their contract if they have written down vital information and conditions. Despite this, there is no legal support or the court system to rely on if there is a fraud, scam, or another unexpected issue [88].

D. SCALABILITY ISSUE

Anyone who wishes to join a blockchain network can join it by becoming a volunteer node. Although maintaining network efficiency and security is challenging as a network grows [150]. The scalability problem in blockchain networks can result in delays and other problems. Several solutions to the Bitcoin blockchain scalability issues have been suggested. However, the authors note that possible delays may not be the only problem. As a new node joins the network, the bootstrap time is the time it takes to download and analyze the network's history, which is quite expensive and takes time for an old and large blockchain like Bitcoin. Further, they examined the following solutions to increase the network's scalability:

-To jam more transactions into a block, the volume of information in each transaction can be reduced

-It is possible to find the optimal block size by adjusting the block size. Scalability issues in blockchain can be categorized into three categories: throughput, cost, and capacity. All transactions performed by a miner are considered to be the capacity of the miner. There is an increase in volume every day. Transaction fees apply to even small transactions [151]. Transactions that are too small in size and, thus, too cheap in fee cause the problem, but too many have to be transmitted over the network. Moreover, throughput problems are experienced by transactions awaiting inclusion in a block. It takes a long time to process small blocks [152].

E. ACCESS CONTROL

It is true that blockchain will always contain a record of previous transactions, and you can expect huge quantities of data to be replicated across all nodes, but that does not make blockchain a database by itself. Large files stored on blockchain could be bloated by these two specifications. The problem is that blockchain storage networks cannot share files among users. Smart contracts-based solutions have been offered to overcome this issue, but they only work for IPFS [153].

F. REPUTATION SYSTEM ISSUES

There is a discussion of the trustworthiness of virtual communities such as Facebook or Twitter. While global reputation systems can reveal recommendations' results, we should note that those results have been derived from the opinions of all nodes, so they might not be reliable, and the other components themselves may not be reliable. In response, they offer a local reputation system that takes only recommendations from the entourage of the user into account. Using blockchain technology, we can implement this idea so that only recommendations from trusted people can be used [154].

G. SWITCHING TO BLOCKCHAIN

There are some instances when blockchain networks may seem to present a problem on first glance, but this is not always the case. There may be a situation in which blockchain networks are not the most appropriate solution for every individual or company. Before implementing a blockchain, it is essential to examine the pros and cons of it so that you can make an informed decision. Therefore, data storage using this method is cheaper and more secure for one individual. Cloud storage is not yet compatible with existing solutions, such as data analysts or processors, so companies should remain cautious. In addition to private blockchains, consortium blockchains can also be developed with the debated technology. Members of these blockchains (e.g., companies) can utilize the blockchain as a collective space instead of storing their personal computers, incurring large hardware costs, or having their data uploaded on external servers. It is possible to customize a blockchain to address a specific characteristic, such as the speed at which stored files are downloaded. Each host must provide a certain amount of storage space to enable such a facility. Nodes with high availability and redundancy should be used when storing high-value data. Quantum computing has a wide range of applications. Authentication, key exchange, and secret key sharing are among the applications. It is possible to generate a group of particles using quantum entanglement instead of sharing as it is currently done in blockchains. Entanglement in quantum mechanics has the critical property of not describing a single particle individually but determining the whole batch's state. Cloud service providers can also use this technology to keep track of all transactions within their network through a chain. It is cheaper than previous models because the data is encrypted before transmission on the network, proofs are sent in fixed intervals, and costs are determined according to usage [155].

VIII. CONCLUSION

In this brief survey we elaborated about the importance of the decentralized storage networks that are intrinsically based on blockchain technologies. Though a lot of studiers are going on in blockchain based storages, still there is a dire need of through investigations on each of these storage networks to assess the suitability of implication according to the use case. Apart from that, due to their decentralized, peer-to-peer nature, blockchains have the potential to make a significant impact on business across many industries. One of our era's most crucial and controversial issues is the storage and retrieval of data in cloud storage. Blockchain-based storage systems overcome several shortcomings of traditional storage systems. Our survey discusses a new way to store data to ensure privacy and security. However, blockchain-based storage remains in its infancy due to scalability, data analysis, and access issues. As with the rest of the new applications of this technology, blockchain-based storage is still in development. Every consensus protocol on a blockchain was built to achieve specific goals, such as speed. Organizations can modify, combine, or create protocols to meet their needs differently.

ACKNOWLEDGMENT

The article processing charge (APC) was funded by the Research Management Centre (RMC), Universiti Malaysia Sabah, through the UMS/PPI-DPJ1 Journal Article Fund.

REFERENCES

[1] X. Zhang, J. Grannis, I. Baggili, and N. L. Beebe, "Frameup: An incriminatory attack on Storj: A peer to peer blockchain enabled distributed storage system," *Digit. Investig.*, vol. 29, pp. 28–42, 2019, doi: 10.1016/j.diin.2019.02.003.

[2] F. Shawn and J. L. Wilkinson, "Metadisk: Blockchain-based decentralized file storage application," *Liq. Cryst.*, vol. 14, no. 2, pp. 573–580, 2014.

[3] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj a peer-to-peer cloud storage network," IPFS, U.K., Tech. Rep., 2016, pp. 1–37.

[4] I. Vakilinia, S. Vakilinia, S. Badsha, E. Arslan, and S. Sengupta, "Pooling approach for task allocation in the blockchain based decentralized storage network," in *Proc. 15th Int. Conf. Netw. Service Manage. (CNSM)*, Oct. 2019, pp. 1–6, doi: 10.23919/CNSM46954.2019.9012719.

[5] A. M. Girgis, O. Ercetin, M. Nafie, and T. ElBatt, "Decentralized coded caching in wireless networks: Trade-off between storage and latency," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 2443–2447.

[6] Z. Kong, S. A. Aly, and E. Soljanin, "Decentralized coding algorithms for distributed storage in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 2, pp. 261–267, Feb. 2010, doi: 10.1109/JSAC.2010.100215.

[7] C. Cai, X. Yuan, and C. Wang, "Towards trustworthy and private keyword search in encrypted decentralized storage," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, Jul. 2017, doi: 10.1109/ICC.2017.7996810.

[8] N. Z. Benisi, M. Aminian, and B. Javadi, "Blockchain-based decentralized storage networks: A survey," *J. Netw. Comput. Appl.*, vol. 162, Jul. 2020, Art. no. 102656, doi: 10.1016/j.jnca.2020.102656.

[9] A. Shah, N. Sheoran, and S. Gupta, "Decentralized storage network with smart contract incentivisation candidate's declaration," Bachelor Technol. Comput. Sci. Eng., Tech. Rep., 2018.

[10] M. Aloqaily, O. Bouachir, A. Boukerche, and I. A. Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," *IEEE Netw.*, vol. 35, no. 1, pp. 64–71, Jan. 2021.

[11] M. Firdaus and K. H. Rhee, "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Appl. Sci.*, vol. 11, no. 1, pp. 1–21, Jan. 2021, doi: 10.3390/app11010414.

[12] N. Lipusch, "Initial coin offerings—A paradigm shift in funding disruptive innovation," *SSRN Electron. J.*, vol. 139, pp. 1–21, Mar. 2018, doi: 10.2139/ssrn.3148181.

[13] S. Yang, A. Hareedy, R. Calderbank, and L. Dolecek, "Topology-aware cooperative data protection in blockchain-based decentralized storage networks," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 1-6.

[14] Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain-empowered decentralized storage in Air-to-Ground industrial networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3593–3601, Jun. 2019, doi: 10.1109/TII.2019.2903559.

[15] A. S. de Pedro, D. Levi, and L. I. Cuende, "Witnet: A decentralized Oracle network protocol," 2017, *arXiv:1711.09756*.

[16] S. He, Y. Lu, Q. Tang, G. Wang, and C. Q. Wu, "Fair peer-to-peer content delivery via blockchain," 2021, *arXiv:2102.04685*.

[17] K. Aldriwish, "A double-blockchain architecture for secure storage and transaction on the Internet of Things networks," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 6, pp. 119–126, 2021, doi: 10.22937/IJCSNS.2021.21.6.16.

[18] M. Campanelli, D. Fiore, N. Greco, D. Kolonelos, and L. Nizzardo, "Vector commitment techniques and applications to verifiable decentralized storage," Elsevier, Tech. Rep., 2020.

[19] I. Vakilinia, W. Wang, and J. Xin, "An incentive-compatible mechanism for decentralized storage network," 2022, *arXiv:2208.09937*.

[20] Y. Du, H. Duan, A. Zhou, C. Wang, M. Ho Au, and Q. Wang, "Enabling secure and efficient decentralized storage auditing with blockchain," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 5, pp. 3038–3054, Oct. 2022, doi: 10.1109/TDSC.2021.3081826.

[21] Protocol Labs, "Filecoin: A decentralized storage network," IEEE, Tech. Rep., 2017, vol. 9, no. 15.

[22] H. Kopp, M. David, F. Hauck, F. Kargl, and B. Christoph, "Design of a privacy-preserving decentralized file storage with financial incentives," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS PW)*, Apr. 2017, pp. 14–22, doi: 10.1109/EuroSPW.2017.45.

[23] A. P. Kryukov and A. P. Demichev, "Decentralized data storages: Technologies of construction," *Program. Comput. Softw.*, vol. 44, no. 5, pp. 303–315, Sep. 2018, doi: 10.1134/S0361768818050067.

[24] J. C. Song, M. A. Demir, J. J. Prevost, and P. Rad, "Blockchain design for trusted decentralized IoT networks," in *Proc. 13th Annu. Conf. Syst. Syst. Eng. (SoSE)*, Jun. 2018, pp. 169–174.

[25] A. Umar, D. Kumar, and T. Ghose, "Blockchain-based decentralized energy intra-trading with battery storage flexibility in a community microgrid system," *Appl. Energy*, vol. 322, Sep. 2022, Art. no. 119544, doi: 10.1016/j.apenergy.2022.119544.

[26] G. Tian, Y. Hu, J. Wei, Z. Liu, X. Huang, X. Chen, and W. Susilo, "Blockchain-based secure deduplication and shared auditing in decentralized storage," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 6, pp. 3941–3954, Dec. 2022, doi: 10.1109/TDSC.2021.3114160.

[27] J. D. Hunt, A. Nascimento, B. Zakeri, J. Jurasz, P. B. Dąbek, P. S. F. Barbosa, R. Brandão, N. J. De Castro, W. L. Filho, and K. Riahi, "Lift energy storage technology: A solution for decentralized urban energy storage," *Energy*, vol. 254, Sep. 2022, Art. no. 124102, doi: 10.1016/j.energy.2022.124102.

[28] H. Gao, N. Bing, H. Xie, and W. Yu, "Energy harvesting and storage blocks based on 3D oriented expanded graphite and stearic acid with high thermal conductivity for solar thermal application," *Energy*, vol. 254, Sep. 2022, Art. no. 124198, doi: 10.1016/j.energy.2022.124198.

[29] L. Wang and Y. Wang, "Supply chain financial service management system based on block chain IoT data sharing and edge computing," *Alexandria Eng. J.*, vol. 61, no. 1, pp. 147–158, Jan. 2022, doi: 10.1016/j.aej.2021.04.079.

[30] C. Wu, Y. Chen, Z. Qi, and H. Guan, "DSPR: Secure decentralized storage with proof-of-replication for edge devices," *J. Syst. Archit.*, vol. 125, Apr. 2022, Art. no. 102441, doi: 10.1016/j.sysarc.2022.102441.
[31] A. Rosini, R. Procopio, A. Bonfiglio, G. P. Incremona, and A. Ferrara, "A decentralized higher order sliding mode control for islanded photovoltaic-storage systems," *Energy*, vol. 255, Sep. 2022, Art. no. 124502, doi: 10.1016/j.energy.2022.124502.
[32] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain-based decentralized architecture for cloud storage system," *J. Inf. Secur. Appl.*, vol. 62, Nov. 2021, Art. no. 102970, doi: 10.1016/j.jisa.2021.102970.
[33] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain technology for cloud storage: A systematic literature review," *ACM Comput. Surveys*, vol. 53, no. 4, pp. 1–32, Sep. 2020, doi: 10.1145/3403954.
[34] A. Sanna, B. Buchspies, M. Ernst, and M. Kaltschmitt, "Decentralized brackish water reverse osmosis desalination plant based on PV and pumped storage—Technical analysis," *Desalination*, vol. 516, Nov. 2021, Art. no. 115232, doi: 10.1016/j.desal.2021.115232.
[35] M. van Roosmalen, A. Herrmann, and A. Kumar, "A review of prefabricated self-sufficient facades with integrated decentralised HVAC and renewable energy generation and storage," *Energy Buildings*, vol. 248, Oct. 2021, Art. no. 111107, doi: 10.1016/j.enbuild.2021.111107.
[36] C. Ziras, A. M. Prostejovsky, H. W. Bindner, and M. Marinelli, "Decentralized and discretized control for storage systems offering primary frequency control," *Electr. Power Syst. Res.*, vol. 177, Dec. 2019, Art. no. 106000, doi: 10.1016/j.epsr.2019.106000.
[37] C. Cai, J. Weng, X. Yuan, and C. Wang, "Enabling reliable keyword search in encrypted decentralized storage with fairness," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 1, pp. 131–144, Feb. 2021, doi: 10.1109/TDSC.2018.2877332.
[38] A. Joshi, H. Kebriaei, V. Mariani, and L. Glielmo, "Decentralized control of residential energy storage system for community peak shaving: A constrained aggregative game," in *Proc. IEEE Madrid PowerTech*, Jun. 2021, pp. 1–6, doi: 10.1109/PowerTech46648.2021.9495052.
[39] Y. Liu and S. Zhang, "Information security and storage of Internet of Things based on block chains," *Future Gener. Comput. Syst.*, vol. 106, pp. 296–303, May 2020, doi: 10.1016/j.future.2020.01.023.
[40] F. Härer and H.-G. Fill, "Decentralized attestation and distribution of information using blockchains and multi-protocol storage," *IEEE Access*, vol. 10, pp. 18035–18054, 2022, doi: 10.1109/ACCESS.2022.3150356.
[41] H. Yu, Q. Hu, Z. Yang, and H. Liu, "Efficient continuous big data integrity checking for decentralized storage," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1658–1673, Jun. 2021, doi: 10.1109/TNSE.2021.3068261.
[42] D. Li and C. Ngai Man Ho, "A module-based plug-n-play DC microgrid with fully decentralized control for IEEE empower a billion lives competition," *IEEE Trans. Power Electron.*, vol. 36, no. 2, pp. 1764–1776, Feb. 2021, doi: 10.1109/TPEL.2020.3009631.
[43] A. Rosini, D. Mestriner, A. Labella, A. Bonfiglio, and R. Procopio, "A decentralized approach for frequency and voltage regulation in islanded PV-storage microgrids," *Electr. Power Syst. Res.*, vol. 193, Apr. 2021, Art. no. 106974, doi: 10.1016/j.epsr.2020.106974.
[44] S. M. Hosseini, R. Carli, J. Jantzen, and M. Dotoli, "Multi-block ADMM approach for decentralized demand response of energy communities with flexible loads and shared energy storage system," in *Proc. 30th Medit. Conf. Control Autom. (MED)*, Jul. 2022, pp. 67–72, doi: 10.1109/MED54222.2022.9837173.
[45] R. Mishra, D. Ramesh, D. R. Edla, and L. Qi, "DS-chain: A secure and auditable multi-cloud assisted EHR storage model on efficient deletable blockchain," *J. Ind. Inf. Integr.*, vol. 26, Mar. 2022, Art. no. 100315, doi: 10.1016/j.jii.2021.100315.
[46] L. Zhaoliang, W. Huang, and D. Wang, "Functional agricultural monitoring data storage based on sustainable block chain technology," *J. Cleaner Prod.*, vol. 281, Jan. 2021, Art. no. 124078, doi: 10.1016/j.jclepro.2020.124078.
[47] R. Ranjan, A. Panchbhai, and A. Kumar, "Decentralized primary control of PV-battery system integrated with DC microgrid in off-grid mode," in *Proc. IEEE Int. Conf. Power Electron., Smart Grid, Renewable Energy (PESGRE)*, Jan. 2022, pp. 1–5, doi: 10.1109/PESGRE52268.2022.9715964.
[48] V. A. Kanade, "A blockchain-based distributed storage network to manage growing data storage needs," in *Proc. 3rd Int. Conf. Signal Process. Commun. (ICPSC)*, May 2021, pp. 365–368, doi: 10.1109/ICSPC51351.2021.9451813.
[49] B. Guidi, A. Michienzi, and L. Ricci, "Data persistence in decentralized social applications: The IPFS approach," in *Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2021, pp. 1–4, doi: 10.1109/CCNC49032.2021.9369473.
[50] Y. Ren, D. Huang, W. Wang, and X. Yu, "BSMD: A blockchain-based secure storage mechanism for big spatio-temporal data," *Future Gener. Comput. Syst.*, vol. 138, pp. 328–338, Jan. 2023, doi: 10.1016/j.future.2022.09.008.
[51] C. B. Costa, A. J. P. Cortez, D. D. Adão, C. M. De Almeida, E. M. Taguchi, I. De Oliveira, J. F. D. O. Santos, A. P. R. Da Rosa, J. T. D. S. Tokunaga, C. P. Arnoni, and F. R. M. Latini, "Optimization of red blood cell unit storage during SARS-COV-2 pandemic: Adopting new strategies to ensure supply in a decentralized blood bank in Brazil," *Hematol., Transfusion Cell Therapy*, vol. 43, no. 3, pp. 229–235, Jul. 2021, doi: 10.1016/j.htct.2021.03.002.
[52] Y. Su, Y. Li, B. Yang, and Y. Ding, "Decentralized self-auditing scheme with errors localization for multi-cloud storage," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2838–2850, Aug. 2022, doi: 10.1109/TDSC.2021.3075984.
[53] G. Goos. (2022). *Founding Editors Editorial Board Members*. [Online]. Available: http://www.springer.com/series/7410
[54] Z. Chen, L. Cui, B. Palanisamy, and L.-J. Zhang, *Blockchain—ICBC*, vol. 12404. Cham, Switzerland: Springer, 2020.
[55] S. Haque, Z. Eberhart, A. Bansal, and C. McMillan, "Semantic similarity metrics for evaluating source code summarization," in *Proc. IEEE/ACM 30th Int. Conf. Program Comprehension (ICPC)*, May 2022, pp. 36–47, doi: 10.1145/nnnnnnn.nnnnnnn.
[56] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," in *Proc. Cloud Comput. Secur. Workshop*, Nov. 2017, pp. 45–50, doi: 10.1145/3140649.3140656.
[57] J. Li, J. Wu, L. Chen, and J. Li, "Deduplication with blockchain for secure cloud storage," in *Commun. Comput. Inf. Sci.*, vol. 2018, vol. 945, pp. 558–570, doi: 10.1007/978-981-13-2922-7_36.
[58] K. Hao, J. Xin, Z. Wang, Z. Jiang, and G. Wang, "Decentralized data integrity verification model in untrusted environment," in *Web and Big Data* (Lecture Notes in Computer Science), vol. 10988. New York, NY, USA: Association for Computing Machinery, 2018, pp. 410–424, doi: 10.1007/978-3-319-96893-3_31.
[59] G. Ateniese, L. Chen, M. Etemad, and Q. Tang, "Proof of storage-time: Efficiently checking continuous data availability," Assoc. Comput. Machinery, New York, NY, USA, Tech. Rep., 2020.
[60] S. Kyun, J. Yi, and J. Jang, "A decentralized approach to education powered by blockchain technology," *Asia–pacific J. Convergent Res. Interchange*, vol. 7, no. 7, pp. 131–141, Jul. 2021, doi: 10.47116/apjcri.2021.07.13.
[61] V. Heidaripour Lakhani, L. Jehl, R. Hendriksen, and V. Estrada-Galiñanes, "Fair incentivization of bandwidth sharing in decentralized storage networks," 2022, *arXiv:2208.07067*.
[62] T. Viet Doan, Y. Psaras, J. Ott, and V. Bajpai, "Towards decentralised cloud storage with IPFS: Opportunities, challenges, and future directions," 2022, *arXiv:2202.06315*.
[63] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, May 2019, doi: 10.3390/app9091736.x.
[64] J. Benet, "IPFS—Content addressed, versioned, P2P file system," 2014, *arXiv:1407.3561*.
[65] H. Chen, Y. Lu, and Y. Cheng, "FileInsurer: A scalable and reliable protocol for decentralized file storage in blockchain," 2022, *arXiv:2207.11657*.
[66] G. Subathra, A. Antonidoss, and B. K. Singh, "Decentralized consensus blockchain and IPFS-based data aggregation for efficient data storage scheme," *Secur. Commun. Netw.*, vol. 2022, pp. 1–13, Jul. 2022, doi: 10.1155/2022/3167958.
[67] H. Wang, Y. Wang, J. Wu, P. Chen, Z. Wu, and G. Yang, "Small-size reconfigurable loop antenna for mobile phone applications," *IEEE Access*, vol. 4, pp. 5179–5186, 2016, doi: 10.1109/ACCESS.2016.2593794.
[68] E. Cecchetti, B. Fisch, I. Miers, and A. Juels, "PIES: Public incompressible encodings for decentralized storage," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 1351–1367, doi: 10.1145/3319535.3354231.
[69] G. Tefera, K. She, and F. Deeba, "Decentralized adaptive latency-aware cloud-edge-dew architecture for unreliable network," in *Proc. ACM Int. Conf. Proc.*, 2019, pp. 142–146, doi: 10.1145/3318299.3318380.
[70] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019, doi: 10.1109/ACCESS.2018.2890736.
[71] H. S. Huang, T. S. Chang, and J. Y. Wu, "A secure file sharing system based on IPFS and blockchain," in *Proc. ACM Int. Conf.*, Jul. 2020, pp. 96–100, doi: 10.1145/3409934.3409948.

[72] D. Francati, G. Ateniese, A. Faye, A. M. Milazzo, A. M. Perillo, L. Schiatti, and G. Giordano, "Audita: A blockchain-based auditing framework for off-chain storage," in *Proc. 9th Int. Workshop Secur. Blockchain Cloud Comput.*, May 2021, pp. 5–10, doi: 10.1145/3457977.3460293.

[73] Y. Zhang, W. You, S. Jia, L. Liu, Z. Li, and W. Qian, "EnclavePoSt: A practical proof of storage-time in cloud via Intel SGX," *Secur. Commun. Netw.*, vol. 2022, pp. 1–16, May 2022, doi: 10.1155/2022/7868502.

[74] Z. Yuan, J. Wu, J. Gong, Y. Liu, G. Tian, and J. Wang, "Blockchain-based self-auditing scheme with batch verification for decentralized storage," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–13, Jun. 2022, doi: 10.1155/2022/6998046.

[75] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020, doi: 10.1109/ACCESS.2020.2988579.

[76] S. He. *Digital Commons @ NJIT Digital Commons @ NJIT Dissertations Electronic Theses and Dissertations Towards Practicalization of Blockchain-Based Decentralized Towards practicalization of Blockchain-Based Decentralized Applications Applications*. [Online]. Available: https://digitalcommons.njit.edu/dissertations/1602

[77] M. Dai, S. Zhang, H. Wang, and S. Jin, "A low storage room requirement framework for distributed ledger in blockchain," *IEEE Access*, vol. 6, pp. 22970–22975, 2018, doi: 10.1109/ACCESS.2018.2814624.

[78] S. P. Gochhayat, S. Shetty, R. Mukkamala, P. Foytik, G. A. Kamhoua, and L. Njilla, "Measuring decentrality in blockchain based systems," *IEEE Access*, vol. 8, pp. 178372–178390, 2020, doi: 10.1109/ACCESS.2020.3026577.

[79] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based Agri-Food supply chain: A complete solution," *IEEE Access*, vol. 8, pp. 69230–69243, 2020, doi: 10.1109/ACCESS.2020.2986257.

[80] O. Hammoud, I. Tarkhanov, and A. Kosmarski, "An architecture for distributed electronic documents storage in decentralized blockchain B2B applications," *Computers*, vol. 10, no. 11, p. 142, Nov. 2021, doi: 10.3390/computers10110142.

[81] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019, doi: 10.1016/j.comcom.2019.01.006.

[82] M. Firdaus and K. Rhee, "Applied sciences on blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Appl. Sci.*, vol. 11, no. 1, p. 414, 2021.

[83] Y. Li, Y. Yu, R. Chen, X. Du, and M. Guizani, "IntegrityChain: Provable data possession for decentralized storage," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1205–1217, Jun. 2020, doi: 10.1109/JSAC.2020.2986664.

[84] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *J. Netw. Comput. Appl.*, vol. 143, pp. 167–177, Oct. 2019, doi: 10.1016/j.jnca.2019.06.019.

[85] I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Implementing decentralized auctions using blockchain smart contracts," *Technol. Forecasting Social Change*, vol. 168, Jul. 2021, Art. no. 120786, doi: 10.1016/j.techfore.2021.120786.

[86] N. Nizamuddin, K. Salah, M. A. Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS," *Comput. Electr. Eng.*, vol. 76, pp. 183–197, Jun. 2019, doi: 10.1016/j.compeleceng.2019.03.014.

[87] Y. Zhang and F. Xi'an, "Multiplication-based pulse integration for detecting underwater target in impulsive noise environment," *IEEE Access*, vol. 4, pp. 6894–6900, 2016, doi: 10.1109/ACCESS.2016.2618375.

[88] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018, doi: 10.1109/ACCESS.2018.2851611.

[89] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018, doi: 10.1109/ACCESS.2018.2870644.

[90] M. Yan, J. Feng, T. G. Marbach, R. J. Stones, G. Wang, and X. Liu, "Gecko: A resilient dispersal scheme for multi-cloud storage," *IEEE Access*, vol. 7, pp. 77387–77397, 2019, doi: 10.1109/ACCESS.2019.2920405.

[91] W. Liang, Y. Fan, K.-C. Li, D. Zhang, and J.-L. Gaudiot, "Secure data storage and recovery in industrial blockchain network environments," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6543–6552, Oct. 2020, doi: 10.1109/TII.2020.2966069.

[92] L. Zhou, L. Wang, and Y. Sun, "MIStore: A blockchain-based medical insurance storage system," *J. Med. Syst.*, vol. 42, no. 8, Aug. 2018, doi: 10.1007/s10916-018-0996-4.

[93] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Top student perspectives on blockchain & Cryptocurrencies," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[94] Y. Hei, Y. Liu, D. Li, J. Liu, and Q. Wu, "Themis: An accountable blockchain-based P2P cloud storage scheme," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 1, pp. 225–239, Jan. 2021, doi: 10.1007/s12083-020-00967-6.

[95] M. Kassen, "Blockchain and e-government innovation: Automation of public information processes," *Inf. Syst.*, vol. 103, Jan. 2022, Art. no. 101862, doi: 10.1016/j.is.2021.101862.

[96] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale Internet of Things data storage and protection," *IEEE Trans. Services Comput.*, vol. 12, no. 5, pp. 762–771, Oct. 2019, doi: 10.1109/TSC.2018.2853167.

[97] M. Debe, K. Salah, M. Habib Ur Rehman, and D. Svetinovic, "IoT public fog nodes reputation system: A decentralized solution using ethereum blockchain," *IEEE Access*, vol. 7, pp. 178082–178093, 2019, doi: 10.1109/ACCESS.2019.2958355.

[98] D. Chen, H. Yuan, S. Hu, Q. Wang, and C. Wang, "BOSSA: A decentralized system for proofs of data retrievability and replication," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 4, pp. 786–798, Apr. 2021, doi: 10.1109/TPDS.2020.3030063.

[99] Y. Cao, W. Wei, L. Wu, S. Mei, M. Shahidehpour, and Z. Li, "Decentralized operation of interdependent power distribution network and district heating network: A market-driven approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5374–5385, Sep. 2019, doi: 10.1109/TSG.2018.2880909.

[100] C. Mcphee, A. Ljutic, H. Rooney, B. Aiken, and M. Rooney, "Editorial: Blockchain a blockchain ecosystem for digital identity: Improving service delivery in Canada's public and private sectors Greg Wolfond Q&A. Is Internal audit ready for blockchain? Technology innovation management review," IEEE, USA, Tech. Rep., 2017, doi: 10.22215/timreview/1107.

[101] Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain-empowered decentralized storage in air-to-ground industrial networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3593–3601, Jun. 2019, doi: 10.1109/TII.2019.2903559.

[102] H. Lutfiyya. *15th International Conference on Network and Service Management; 1st International Workshop on Analytics for Service and Application Management (AnServApp 2019); International Workshop on High-Precision Networks Operations and Control, Segment Routing and Service Function Chaining (HiP Net+SR/SFC 2019)*, IEEE Xplore, Halifax, Canada, Oct. 2019.

[103] M. S. Sonkor and B. G. De Soto, "Towards secure construction networks: A data-sharing architecture utilizing blockchain technology and decentralized storage," in *Proc. Construct. Blockchain Consortium Conf.*, Feb. 2022, pp. 20–22, doi: 10.47330/cbc.2021.nokh7555.

[104] M. Krichen, M. Ammi, A. Mihoub, and M. Almutiq, "Blockchain for modern applications: A survey," *Sensors*, vol. 22, no. 14, p. 5274, Jul. 2022, doi: 10.3390/s22145274.

[105] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Appl. Sci.*, vol. 10, no. 6, p. 2011, Mar. 2020, doi: 10.3390/app10062011.

[106] L. Jiang and X. Zhang, "BCOSN: A blockchain-based decentralized online social network," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1454–1466, Dec. 2019, doi: 10.1109/TCSS.2019.2941650.

[107] C. Xie, Y. Sun, and H. Luo, "Secured data storage scheme based on block chain for agricultural products tracking," in *Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2017, pp. 45–50, doi: 10.1109/BIGCOM.2017.43.

[108] Y. Xu, "Section-blockchain: A storage reduced blockchain protocol, the foundation of an autotrophic decentralized storage architecture," in *Proc. 23rd Int. Conf. Eng. Complex Comput. Syst. (ICECCS)*, Dec. 2018, pp. 115–125, doi: 10.1109/ICECCS2018.2018.00020.

[109] O. F. Cangir, O. Cankur, and A. Ozsoy, "A taxonomy for blockchain based distributed storage technologies," *Inf. Process. Manage.*, vol. 58, no. 5, Sep. 2021, Art. no. 102627, doi: 10.1016/j.ipm.2021.102627.

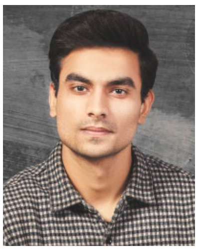
[110] P. Banerjee, C. Govindarajan, P. Jayachandran, and S. Ruj, "Reliable, fair and decentralized marketplace for content sharing using blockchain," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 365–370, doi: 10.1109/Blockchain50366.2020.00053.

[111] *IEEE Information Theory Society and Institute of Electrical and Electronics Engineers, 2020 IEEE International Symposium on Information Theory: Proceedings*, Los Angeles, CA, USA, Jul. 2020.

[112] S. Ali, G. Wang, B. White, and R. L. Cottrell, ''A blockchain-based decentralized data storage and access framework for PingER,'' in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1303–1308, doi: 10.1109/TrustCom/BigDataSE.2018.00179.
[113] B. Fisch, J. Bonneau, N. Greco, and J. Benet. (2018). *Scaling Proof-of-Replication for Filecoin Mining*. [Online]. Available: https://web.stanford.edu/ bfisch/porep_short.pdf
[114] *3rd International Conference on Communication and Electronics Systems (ICCES)*, IEEE Xplore, Los Angeles, CA, USA, 2018.
[115] Y. Gu, D. Hou, X. Wu, J. Tao, and Y. Zhang, ''Decentralized transaction mechanism based on smart contract in distributed data storage,'' *Information*, vol. 9, no. 11, p. 286, Nov. 2018, doi: 10.3390/info9110286.
[116] T. G. Jiang, H. Fang, and H. Wang, ''Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis,'' *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019, doi: 10.1109/JIOT.2018.2874398.
[117] R. Paul. *Institute of Engineering & Management, Institute of Electrical and Electronics Engineers. Vancouver Section, and Institute of Electrical and Electronics Engineers, The 11th Annual IEEE Information Technology, Electronics and Mobile Communication Conference: Virtual Conference*, Vancouver, BC, Canada, Nov. 2020.
[118] S. Chakrabarti. *Institute of Electrical and Electronics Engineers, and I. Institute of Engineering & Management (Kolkata, 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Univ. British Columbia, Vancouver, BC, Canada, Nov. 2018.
[119] O. Choudhury, H. Sarker, N. Rudolph, M. Foreman, N. Fay, M. Dhuliawala, I. Sylla, N. Fairoza, and A. K. Das, ''Enforcing human subject regulations using blockchain and smart contracts,'' *Blockchain Healthcare Today*, Mar. 2018, doi: 10.30953/bhty.v1.10.
[120] H. Al Breiki, L. Al Qassem, K. Salah, M. H. Ur Rehman, and D. Sevtinovic, ''Decentralized access control for IoT data using blockchain and trusted Oracles,'' in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Nov. 2019, pp. 248–257, doi: 10.1109/ICII.2019.00051.
[121] *Universidad Autónoma del Perú, Institute of Electrical and Electronics Engineers, and Institute of Electrical and Electronics Engineers. Peru Section, Proceedings of 2019 IEEE XXVI International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, Lima, Peru, pp. 12–14, Aug. 2019.
[122] H. Rathore, A. Mohamed, and M. Guizani, ''A survey of blockchain enabled cyber-physical systems,'' *Sensors*, vol. 20, no. 1, p. 282, Jan. 2020, doi: 10.3390/s20010282.
[123] *SCAD College of Engineering and Technology and Institute of Electrical and Electronics Engineers, Proceedings of the 4th International Conference on Trends in Electronics and Informatics (ICOEI 2020)*, IEEE, Orlando, FL, USA, Jun. 2020.
[124] F. Aminifar, M. Fotuhi-Firuzabad, A. Safdarian, A. Davoudi, and M. Shahidehpour, ''Synchrophasor measurement technology in power systems: Panorama and state-of-the-art,'' *IEEE Access*, vol. 2, pp. 1607–1628, 2014, doi: 10.1109/ACCESS.2015.2389659.
[125] A. Abdelmaboud, A. I. A. Ahmed, M. Abaker, T. A. E. Eisa, H. Albasheer, S. A. Ghorashi, and F. K. Karim, ''Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions,'' *Electronics*, vol. 11, no. 4, p. 630, Feb. 2022, doi: 10.3390/electronics11040630.
[126] *IEEE Communications Society and Institute of Electrical and Electronics Engineers, IEEE INFOCOM 2018—IEEE Conference on Computer Communications*, IEEE, Tamil Nadu, India, 2018.
[127] *Institute of Electrical and Electronics Engineers, 2017 IEEE International Symposium on Information Theory (ISIT)*, IEEE, USA, Jun. 2017.
[128] S. Ølnes, J. Ubacht, and M. Janssen, ''Blockchain in government: Benefits and implications of distributed ledger technology for information sharing,'' *Government Inf. Quart.*, vol. 34, pp. 355–364, Sep. 2017, doi: 10.1016/j.giq.2017.09.007.
[129] *IEEE Staff, 2017 IEEE International Conference on Communications (ICC)*, IEEE, 2017.
[130] V.-D. Pham, C. T. Tran, T. Nguyen, T. T. Nguyen, B. L. Do, T. C. Dao, and B. M. Nguyen. (2020). *B-box—A Decentralized Storage System Using IPFS, Attributed-based Encryption, and Blockchain*. [Online]. Available: https://v-chain.vn/solutions/b-box
[131] G. Ayoade, V. Karande, L. Khan, and K. Hamlen, ''Decentralized IoT data management using BlockChain and trusted execution environment,'' in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Jul. 2018, pp. 15–22, doi: 10.1109/IRI.2018.00011.
[132] Q. Zheng, Y. Li, P. Chen, and X. Dong, ''An innovative IPFS-based storage model for blockchain,'' in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI)*, Dec. 2018, pp. 704–708, doi: 10.1109/WI.2018.000-8.
[133] M. Ali, R. Shea, and M. J. Freedman, ''Blockstack: A new decentralized internet,'' IEEE, Ho Chi Minh City, Vietnam, Tech. Rep., 2017, pp. 1–22.
[134] *M. IEEE Systems, IEEE Reliability Society, and Institute of Electrical and Electronics Engineers, 2018 13th System of Systems Engineering Conference (SoSE)*, Sorbonne Universite Campus Pierre et Marie Curie, Paris, France, Jun. 2018.
[135] T. Hepp, M. Sharinghousen, P. Ehret, A. Schoenhals, and B. Gipp, ''On-chain vs. off-chain storage for supply- and blockchain integration,'' *J. Inf. Technol.*, vol. 60, nos. 5–6, pp. 283–291, Dec. 2018, doi: 10.1515/itit-2018-0019.
[136] Y. Du, H. Duan, A. Zhou, C. Wang, M. Ho Au, and Q. Wang, ''Towards privacy-assured and lightweight on-chain auditing of decentralized storage,'' in *Proc. IEEE 40th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Dec. 2020, pp. 201–211, doi: 10.1109/ICDCS47774.2020.00023.
[137] A. Shah, N. Sheoran, S. Gupta, M. Mishra, and S. Gangopadhyay, ''Decentralized storage network with smart contract incentivisation computer science and engineering,'' IEEE, Paris France, Tech. Rep., 2018.
[138] S. M. Danish, K. Zhang, and H.-A. Jacobsen, ''BlockAM: An adaptive middleware for intelligent data storage selection for Internet of Things,'' in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPS)*, Aug. 2020, pp. 61–71, doi: 10.1109/DAPPS49028.2020.00007.
[139] P. S. Austria, ''Analysis of blockchain-based storage systems,'' Assoc. Comput. Machinery, New York, NY, USA, Tech. Rep., 2020.
[140] R. Kothari, B. Jakheliya, and V. Sawant, ''Implementation of a distributed P2P storage network,'' in *Proc. IEEE Int. Conf. Innov. Technol. (INOCON)*, Nov. 2020, doi: 10.1109/INOCON50539.2020.9298375.
[141] *Challenges With Storing Content on Blockchains and DLTs*. [Online]. Available: https://ipfs.io/
[142] R. Schumi, Y. Ranka, J. Bagrecha, K. Gandhi, B. Sarvaria, and P. Chawan, ''A survey on file storage & retrieval using blockchain technology,'' *Int. Res. J. Eng. Technol.*, vol. 5, no. 10, p. 763, 2008. [Online]. Available: https://www.irjet.net/
[143] P.-H. Ko, Y.-L. Hsueh, and C.-W. Hsueh, ''A low-storage blockchain framework based on incentive pricing strategies,'' *FinTech*, vol. 1, no. 3, pp. 250–275, Sep. 2022, doi: 10.3390/fintech1030020.
[144] B. Produit, ''Using blockchain technology in distributed storage systems,'' IPFS Labs, China, Tech. Rep., 2018.
[145] S. Vimal and S. K. Srivatsa, ''A new cluster P2P file sharing system based on IPFS and blockchain technology,'' *J. Ambient Intell. Humanized Comput.*, vol. 23, pp. 1–7, Sep. 2019, doi: 10.1007/s12652-019-01453-5.
[146] G. Wang, Z. Shi, M. Nixon, and S. Han, ''ChainSplitter: Towards blockchain-based industrial IoT architecture for supporting hierarchical storage,'' in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 166–175, doi: 10.1109/Blockchain.2019.00030.
[147] D. Andriesse, A. Slowinska, and H. Bos, ''Compiler-agnostic function detection in binaries,'' in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS P)*, Apr. 2017, pp. 177–189, doi: 10.1109/EuroSP.2017.11.
[148] D. Li, R. Du, Y. Fu, and M. Ho Au, ''Meta-key: A secure data-sharing protocol under blockchain-based decentralized storage architecture,'' *IEEE Netw. Lett.*, vol. 1, no. 1, pp. 30–33, Mar. 2019, doi: 10.1109/lnet.2019.2891998.
[149] B. Fisch, J. Bonneau, N. Greco, and J. Benet, ''Scaling proof-of-replication for filecoin mining,'' IEEE,Seoul, South Korea, Tech. Rep., 2018.
[150] E. Karaarslan and E. Adiguzel, ''Blockchain based DNS and PKI solutions,'' *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 52–57, Sep. 2018, doi: 10.1109/MCOMSTD.2018.1800023.
[151] Y.-J. Han and G.-H. Kim, ''A Comparative Study on Decentralized Storage Platforms for Self-sovereign Dat,'' *Asia–Pacific J. Converg. Res. Interchang.*, vol. 6, no. 5, pp. 1–10, May 2020, doi: 10.21742/apjcri.2020.05.01.
[152] K. R. Ozyilmaz and A. Yurdakul, ''Designing a blockchain-based IoT with ethereum, swarm, and LoRa: The software solution to create high availability with minimal security risks,'' *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 28–34, Mar. 2019.
[153] S. P. Burger, J. D. Jenkins, S. C. Huntington, and I. J. Perez-Arriaga, ''Why distributed?: A critical review of the tradeoffs between centralized and decentralized resources,'' *IEEE Power Energy Mag.*, vol. 17, no. 2, pp. 16–24, Mar. 2019.
[154] Q. Xu, Z. Song, R. Siow, M. Goh, and Y. Li, ''Building an ethereum and IPFS-based decentralized social network system,'' in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 1–6.

[155] B. Vasanthi and M. B. Suresh, "A survey on security and privacy issues of decentralized cloud storage," IEEE, Tech. Rep., 2021, vol. 8, no. 2, doi: 10.36893.DRSR.2021.V08I14.147-151.

MUHAMMAD IRFAN KHALID received the bachelor's degree in software engineering from Government College University Faisalabad (GCUF), in 2017, and the master's degree in software engineering from Bahria University, Islamabad, in 2019. He is currently pursuing the Ph.D. degree with the Department of Information and Electrical Engineering and Applied Mathematics, University of Salerno, Fisciano, Italy. After that, he worked as a Lecturer at the Department of Information Technology, University of Sialkot, for two years. His research interests include cyber security, blockchain technologies, and cryptography for patient data security and privacy.



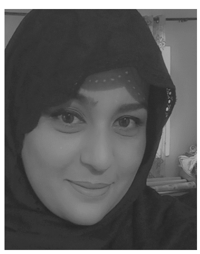
IBTISAM EHSAN received the bachelor's degree in information technology from the University of Sialkot, Sialkot, Pakistan, in 2022, with major subjects like blockchain, cloud computing, the IoT, operating systems, and data base administration. He is currently pursuing the master's degree, with a focus on the IoT and blockchain technology.

AYMAN KHALLEL AL-ANI received the Ph.D. degree in advance computer network from Universiti Sains Malaysia (USM). He is currently a Senior Lecturer with the Faculty of Computing and Informatics, Universiti Malaysia Sabah (UMS). His current research interests include malware detection, web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, the Internet of Things (IoT), IPv6 security, artificial intelligence, machine learning, data mining, and optimization algorithms.

JAWAID IQBAL received the Ph.D. degree from Hazara University, Mansehra, in 2021. He has been teaching at university level for more than nine years. He started his career from the IT Department, Hazara University, in 2013. He also worked at different universities, like the Abbottabad University of Science and Technology (AUST) and the University of Sialkot. Currently, he is working as an Assistant Professor with the Department of Computer Science, Capital University of Science and Technology (CUST), Islamabad. He has taught various subjects of computer science at bachelor's and M.S. program-levels. He has numerous publications in international conferences and journals. His research interests include information security and networks. He is also a member of the Advance Network and Security Research Group, CUST.

SADDAM HUSSAIN received the bachelor's degree from Islamia College, Peshawar, in 2017, and the master's degree from Hazara University Mansehra, in 2021. He is currently pursuing the Ph.D. degree with the School of Digital Science, Universiti Brunei Darussalam. He is a highly motivated and dedicated researcher with a passion for exploring the latest advancements in cryptography, network security, NDN, and wireless sensor networking. With a strong academic background and a wealth of experience, he has published several articles in reputed journals, such as IEEE Access, *Journal of Information Security and Applications* (Elsevier), *Cluster Computing*, *Computer Communications*, IEEE Internet of Things Journal, Hisndawi journals, *CMC*, and MDPI journals. His research interests include various cutting-edge technologies, such as the IoT, the IIoT, quantum computing, cloud computing, information-centric networking, blockchain, and edge computing. He is also actively serving as a Reviewer for reputed journals, including IEEE Access journals, MDPI journals, *International Journal of Wireless Information Networks*, *Scientific Journal of Electrical, Computer, and Informatics Engineering*, and *CMC*.

SYED SAJID ULLAH received the master's (M.S.) degree in computer science from Hazara University Mansehra, Pakistan. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Villanova University, Villanova, PA, USA. He is also working as a Researcher with the National Institute of Standards and Technology (NIST) in the projects, viz.practical implementation of quantum cryptography and security solutions for future internet architecture named data networking. His research interests include cryptography, network security, information-centric networking (ICN), named data networking (NDN), and the IoT.



NAYAB received the bachelor's (B.S.) and master's (M.S.) degrees in computer science from Hazara University Mansehra, Pakistan. She is currently pursuing the Ph.D. degree with The University of Haripur (UoH). She is also an Assistant Professor with GGDC Kakul Abbottabad, Pakistan. Her research interests include cryptography, network security, wireless sensor networking (WSN), information-centric networking (ICN), named data networking (NDN), smart grid, the Internet of Things (IoT), the IIoT, quantum computing, cloud computing, and edge computing.