Journal Pre-proof

Blockchain-based decentralized storage networks: A survey

Nazanin Zahed Benisi, Mehdi Aminian, Bahman Javadi

PII: S1084-8045(20)30130-2

DOI: https://doi.org/10.1016/j.jnca.2020.102656

Reference: YJNCA 102656

To appear in: *Journal of Network and Computer Applications*

Received Date: 6 September 2019

Revised Date: 14 February 2020

Accepted Date: 1 April 2020

Please cite this article as: Benisi, N.Z., Aminian, M., Javadi, B., Blockchain-based decentralized storage networks: A survey, *Journal of Network and Computer Applications* (2020), doi: https://doi.org/10.1016/j.jnca.2020.102656.

Blockchain-Based Decentralized Storage Networks: A Survey

Nazanin Zahed Benisi[1], Mehdi Aminian[1 (*)], Bahman Javadi[2]

[1] Department of Electrical and Computer Engineering, Islamic Azad University, North Tehran Branch, Tehran, Iran
n.zahedbenisi@iau-tnb.ac.ir
m.aminian@iau-tnb.ac.ir
[2] School of Computer, Data and Mathematical Sciences, Western Sydney University, Australia
b.javadi@westernsydney.edu.au

(*) Corresponding author at: Department of Electrical and Computer Engineering, Islamic Azad University, North Tehran Branch, Tehran, Iran
E-mail address: m.aminian@iau-tnb.ac.ir (M. Aminian)

Abstract. *Blockchain* is a new approach to create a distributed network which was first introduced in 2008. By the help of this disruptive technology a peer-to-peer network can be formed where nodes have to reach a consensus and form a chain from accepted blocks, while no central party or trusted controller is required. Among all the existing uses of this technology, decentralized storage systems are one of its prominent applications. Decentralized storage networks, are consisted of a group of people willing to rent out their unused hardware storage space. By implementing end-to-end encryption clients can securely transmit their files through a fully decentralized network and eliminate the risk of data failures that arise from centralized controls. In this network, storage providers are required to prove that they store unaltered files during the time. Also a smart contract between two parties is set out in which rental duration and cost that the customer needs to pay for using that storage space is clarified. This paper presents a comprehensive survey on the blockchain-based storage systems and how they work and then compares them with cloud-based storage networks. Also different techniques of consensus protocols in each group are explored. Next, we have an overview on the advantages and also weak points of blockchain-based storage systems. Finally, we discuss about future research directions.

Keywords: Blockchain, Decentralized Storage, Peer-to-peer Network, Decentralized Network, Cloud Storage.

1 Introduction

Electronic devices such as computers, smartphones and cameras produce enormous volumes of data each day, which require more and more storage resources. In order to

fulfill this necessity, cloud storage systems were created. A Cloud storage system is a cooperation storage service system with multiple devices, many application domains and service forms. Cloud storage is less costly and more reliable than local storage and is less prone to data-loss [1]. The act of storing user's data on memories maintained and secured by a third party is termed cloud storage. To put it simply, data is being stored in the memory of remote devices instead of data owner's hardware [2].

Although one of the greatest innovations in the field of computing is storage and access of data in the cloud, there are many security and availability issues regarding this technology [3]. One of the main problems with cloud storage is lack of transparency and control over stored data. In other words, users are unaware of the exact location where their data is being stored, how and when it is processed or even whether their data has been lost or compromised. Another issue with such systems is lack of trust. Since it is not customary for users and service providers to sign an official contract, there is no legal framework for users to claim compensation if their data is damaged, compromised or sold to third-party companies. In addition, clients are not convinced whether their data is copied or sold elsewhere.

Due to the inherent nature of the cloud, its security flaws cannot be fully resolved despite the enhanced security solutions developed in the past few years. However, a new model for storage systems built on blockchain can effectively overcome these security concerns. Blockchain-based decentralized storage networks let users rent out their unused disk space to those others who need extra storage space.

As shown in [4], aggregation of all unused space on average computer users is more than all Google's storage space as a centralized company with huge storage capacity. It can be concluded that if the unused storage space of computers were aggregated, the whole centralized cloud computing industry would be only a small fraction of the users' collective storage space, and blockchain networks can offer people more storage capacity with lower cost.

In Section 2 of this paper a brief history of distributed file systems, blockchain technology, and in particular, Bitcoin and Ethereum blockchains is provided. In Section 3, four well-known decentralized storage systems and also the research context will be studied. In Section 4 merits of decentralized storage systems are discussed. Section 5 is devoted to open challenges/questions and future research on this topic while Section 6 presents the conclusion of this research.

2 BACKGROUND

2.1 DISTRIBUTED FILE SYSTEMS

In [5] a wide range of definitions toward distributed networks are being discussed. One of the main features of these network architectures, labeled peer-to-peer, is sharing resources such as content, storage and CPU power among others. Some of the advantages of distributed file systems are fault tolerance, availability, scalability and performance [6]. To meet aforementioned benefits, thousands of servers must cooperate with each other and execute users' applications tasks. Plenty of applications such as Hadoop File System (HDFS), CernVM File System (CVFMS), Andrew File

System (AFS), Bigtable and OceanStore offer distributed file system and storage, each with a distinct purpose. Distributed storage file systems use two main techniques to increase data availability and reduce data loss: First method is called replication. This method is fast and straightforward but poses certain challenges such as large storage overhead. In addition, for replication to be effective, the files must be distributed across various domains so as to avoid multiple data failures. The second method is erasure code, which can solve the problem of huge overheads by computational complexity [7-9].

Distributed file storage systems are built on blockchain technology and as such do not have a trusted central party that controls the network. Therefore they are more secure than other types of data storage. In the following subsections blockchain technology and blockchain-based storage systems will be fully covered.

2.2 BLOCKCHAIN

Blockchain is a peer-to-peer network which serves as a public ledger. With the help of a peer-to-peer architecture, networks gain the ability to self-organize, scale and function even in the presence of computer/network failures and remarkably transient population of nodes, without a central server and the overhead of its administration being required (Figure 1) [5].

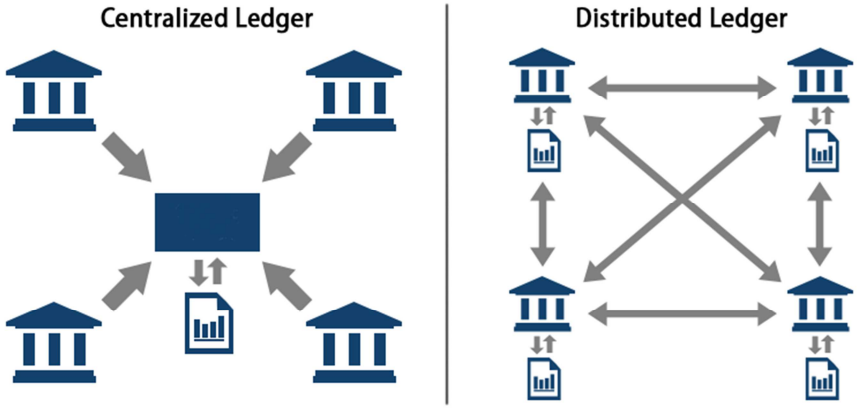

Figure 1 - Centralized network vs. distributed network [10]

Blockchain is a list of connected blocks, each containing a number of a transactions. In fact, the history of all transactions is stored in the blockchain, making it very difficult to tamper. The first block created with no parent is called the genesis block [11]. The process in which transactions are verified by solving a computationally difficult puzzle and finding a specific nonce is called mining. Once the blockchain users have reached a consensus on the validity of a group of transactions through a certain method [12, 13], a new block will be created and added

to the blockchain (Figure 2). A block can only hold vital information and cannot be used as a database.

There are three types of blockchains:

1. Public Blockchain: Any person can join this network and all nodes have equal authority.
2. Private Blockchain: Usually belongs to an organization and permissions can be public or restricted.
3. Consortium Blockchain: Consisted of group of selected nodes (for example a junction of two or more organizations) and permissions can be public or restricted.

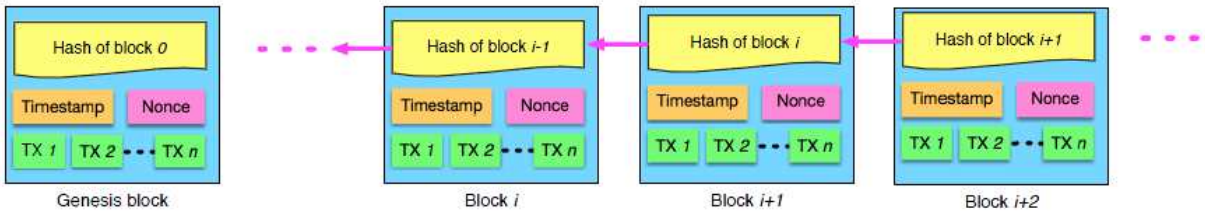

Figure 2 - A sequence of blocks [11]

Consensus Protocol is the act of verifying a transaction in a public ledger. In [14] two main categories of consensus algorithms are described and compared with each other. The first group consists of vote-based consensus algorithms, which are believed to provide better solutions for private and consortium blockchains as their decentralization degree, number of nodes and security threats are lower than public blockchains. In vote-based algorithms, nodes negotiate to make an agreement whether to add a new block to the network. The second group consists of proof-based algorithms. Proof-based algorithms are appropriate for public blockchains, where security threats are higher. Using this method can make a network more trustworthy. In these networks, usually, any number of nodes can freely join the network. Nodes are required to show they have performed sufficient proof and made a block ready to be added to the chain. In return they will be rewarded.

Table 1. Study of Different Consensus Algorithms

Protocol Type	Designated	Required Resources	Implementations
Proof of Work (PoW)	permissionless public distributed ledger	computational resources or hash rate	Bitcoin, Litecoin, ZCash, Monero & …
Proof of Stake (PoS)	permissioned public distributed ledger	requires no special computing power	Ethereum, Neo, Peercoin, Dash and …

Proof of Elapsed Time (PoET)	permissionless public distributed ledger	similar to PoW but it uses much less computational resources	Hyperledger Sawtooth
Proof of Space (PoSpace) / Proof of Capacity (PoC)	public distributed ledger	consumes free disk storage	Burstcoin, SpaceMint
Proof of Retrievability (PoR)	public distributed ledger	consumes free disk storage	Storj
Practical Byzantine Fault Tolerant (PBFT)	permissioned private distributed ledger	minimum computational power or hash rate	Hyperledger Fabric, Stellar, Ripple
Tangle	permissionless public distributed ledger	minimum computational power	IOTA

Wahab and W. Memood [13] did a comprehensive research on consensus protocols. In addition to Proof of Work (PoW) and Proof of Stake (PoS), Proof of Elapsed Time, Proof of Space, Proof of Retrievability, Practical Byzantin Fault Tolerant and also Tangle are introduced and analyzed. Moreover, pros, cons and use cases of each one is explained. Table 1 shows a brief summary of their research.

Key characteristics of blockchain are decentralization, persistency, anonymity and auditability [11]. This technology can be applied in many fields. Some of the most prominent platforms and foundations in various sectors are listed below:

- Banking and financial services: Bitcoin [10], Ethereum [15]
- Healthcare systems [16]: Tierion [17]
- Internet of things (IoT) [18, 19]
- Reputation systems: DREP (Decentralized Reputation System) [20]
- Supply chain management [21]: Ambrosus (AMB) [22], Origin Trail [23], VeChain (VET) [24]
- Insurance: Aeternity [25]
- Prediction and forecasting: Augur [26]
- Private transport and ridesharing: iRide [27]
- Voting: Follow my vote [28]
- Charity and donation: BitGive [29] , One+ One [30]
- Online music [31]: Mycelia, Ujo music
- Energy management: Grid+ [32]
- Retail: OpenBazaar [33]
- Crowdfunding: YouToken [34]
- Cloud storage: Storj [4], Sia [35], FileCoin [36], Swarm [37]

One of the greatest applications of this technology is distributed storage Systems. They are considered a more effective solution for data storage comparing to cloud-based systems due to secure nature of Blockchain. In the following sections existing

blockchain-based storage networks, their use cases as well as advantages and disadvantages of this method will be discussed. Table-2 shows a brief comparison of some metrics between centralized and decentralized storage systems.

Table 2. Centralized Storage Networks vs. Blockchain-Based Storage Systems

Storage Type	Open Source	Scalability	Privacy	Payment Method	Data Processing	Cost	Ability to Choose Hardware Type
Cloud Storage Networks	No	High	Low	Fiat Money	Yes	High	No
Blockchain-based Storage Systems	Yes	Complicated	High	Cryptocurrency	No	Low	Yes

2.3 BITCOIN

Bitcoin is the first blockchain ever created [10]. It came to begin in 2008 and its first block was mined in 2009. The aim of this peer-to-peer electronic cash system was setting financial transactions without going through a financial institution. All transactions are being signed before being transmitted on the network, so as to be identifiable. The history of all transactions will be stored in a Merkle tree [38] (Figure 3). Each block's hash must be calculated before being added to the network. Whereas the hash of each transaction is also written in the next block, each new block changes the Merkle root [38], which automatically confirms the history of the whole blockchain. Though, we have to keep in mind that a hash function (SHA-256) is applied to all entries, which turns outputs to a specific length.

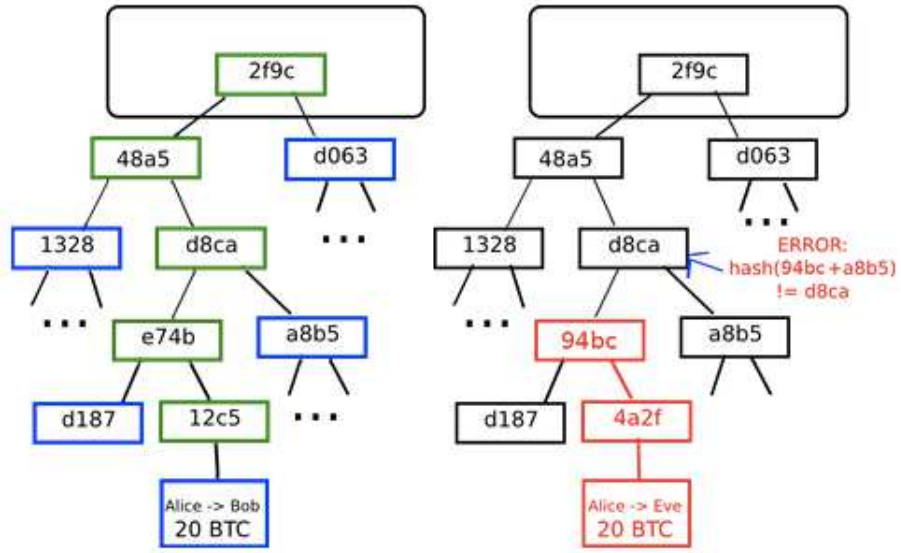

Figure 3- How Merkle Tree Works [15, 38]

Each block has a timestamp, which is the time at which that block is accepted by the network. This prevents the users from spending the same funds twice (also known as double-spending). Moreover, Satoshi's blockchain [10] represented a new approach to privacy. On the one hand, in a blockchain, each person assigns a public key that is visible to all nodes in the network. On the other hand, each person has a private key, which is their bitcoin wallet. As long as users keep their private key securely, it will not be possible to reveal their true identity (Figure 4). In other words, unlike traditional systems, a central party can retrieve a user's identity neither by knowing their public key nor private. The traded cryptocurrency in this blockchain is also called bitcoin and goes by the ticker "BTC".

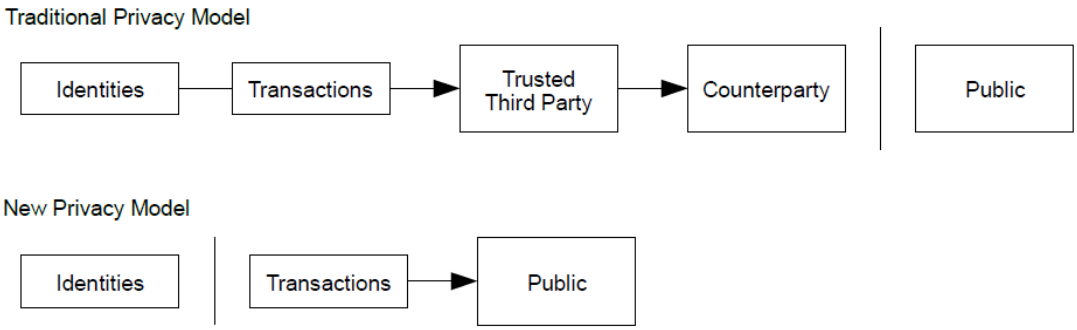

Figure 4 - Traditional privacy model vs. bitcoin privacy model [10]

2.4 ETHEREUM

Ethereum [15] is another open source public blockchain that was developed in 2013 and became available to the public in 2015. Ethereum is an open source public blockchain platform that has two unique features:

- Ethereum allows developers to run their *distributed applications (Dapps)* on Ethereum blockchain. Dapps are consensus-based applications and are resilient to network failures.
- Developers also have the privilege to write *smart contracts* in this network. Smart contracts are a group of codes that can read other codes and make decisions. They are completely discussed in Section 2.5.

Comparing to Bitcoin, transactions are mined faster in Ethereum and the native cryptocurrency of Ethereum is Ether.

2.5 SMART CONTRACTS

Smart contracts are self-executing contracts that consist of a group of codes defining the rules governing transactions and are built on top of an underlying cryptocurrency platform. Users can create their own contracts by writing up the logic in a few lines of code in order to transferring their digital assets without third parties according to arbitrary pre-specified rules. Smart contracts will by default operate as long as there is money in circulation in the network unless they are specifically programmed to self-destruct given certain criteria are met. Smart contracts also are trackable and irreversible [15, 39]. It may sound easy for programmers to write the code and run their smart contract, however, it can end up to a huge money loss whereas the coin/tokens with real value are traded on the platform. Thus, the programmers should have economic knowledge and thinking to be able to write the code that can assure fairness for both parties [39].

3 DISTRIBUTED STORAGE

As noted earlier, one of the applications of blockchain is distributed data storage. Given the problems and limitations of the cloud, programmers have taken a new approach to file storage. In the following sections, four well-known blockchain-based storage systems will be studied. Followed by some research work to address the exiting challenges.

3.1 STORJ

According to [40], it's time for cloud storage systems to become a real cloud. And that's only possible when a massive amount of resources are connected in order to form a storage system. With the advent of blockchain, implementation of this idea became possible. In this platform ordinary people share their unused storage hardware space. Storj configures a trust-based cloud storage system between clients and hosts. All clients' data must be encrypted before transmitting on the network.

Considering the fact that people may want to store massive files, storing all data on the blockchain can cause a problem called *bloating*. To solve this problem, only the metadata of each block is stored on blockchain. Metadata holds some essential information, such as a file's location and its hash. Like any other data on the blockchain, metadata must also be encrypted.

Storj uses Ethereum blockchain and stores the metadata in Satoshi style, enabling users to retrieve their information in full whenever needed. An application called Metadisk runs on the Storj platform and checks the network periodically to make sure the files stored are available and untampered. Each file is stored in at least three locations with the option of increasing this amount to meet the client's demands. As a result, even if the original file is destroyed, the data can still be retrieved through one of the copies. If a node or an audit is not available, another copy of the file would be saved on a new node (Figure 5). This process is called proof-of-redundancy [4].

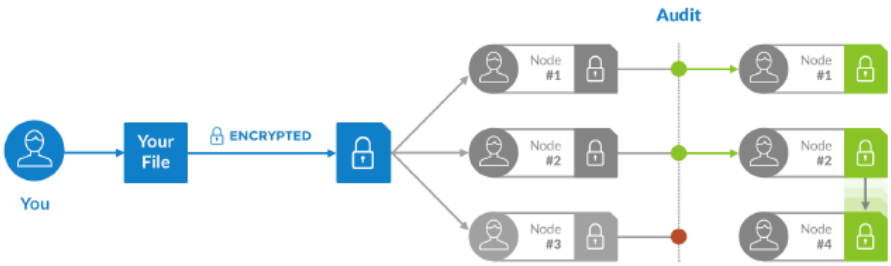

Figure 5 - Recovery from other sources [4]

In Storj all files are split into small fractions before being sent on the network. These small fractions are called *shards* and the process of splitting data into smaller parts is called sharding. With the help of sharding, no single node will have access to a complete copy of a file uploaded on the network. Shards can even be combined with each other when a client is sending smaller files as it helps having them verified at once. Moreover, when important data is being transmitted on the network, sharding can help conceal them by blending them with unnecessary information.

Proof of Space (PoS), also known as Proof of Storage or Proof of Capacity (PoC) is, the consensus protocol used in Storj. The amount of dedicated free space of each miner, has a direct connection to their influence on the network [13]. As noted before, farmers (node that store data on their hardware) are requested to prove that the stored data are available and untampered. Proof-of-storage can be accomplished with two methods:

- Proof -of-storage via Merkle audits [38]
- Proof-of-storage via pre-generated audits

The written contract between the client and the farmer states the fees agreed between the parties for the service. The client will then pay the fees in Storjcoin X (or SJCX) to the service provider according to the smart contract.

Storj V3 [41] has focused on building a platform compatible with the most widely deployed public cloud at the time of paper's publication which is Amazon Web Services. Amazon's first cloud services product is Amazon Simple Storage Service (or Amazon S3). Compatibility should not be restricted to API but functionality, performance, durability, security and privacy are included too. In addition, data replication for increasing availability that is used in many distributed storage networks is questioned in this version and Storj creators believe the best solution of increasing data availability is erasure coding. The possibility of implementing a test network in this version is also provided. Storj test network enables us to run all storage network components locally, make changes and run the network to check the results.

3.2 SIA

Sia is another blockchain-based storage platform [35]. Like Storj, in Sia peers rent out their hardware capacity. Storage providers are known as hosts in this network.

Storage proofs, containing a list of hashes from the file and a fraction of the original file, are publicly available and verifiable therefor the client do not need to verify them personally.

Similar to Storj, data in Sia must be encrypted and digitally signed before submitting in the network. Also, a contract has to set up between the client and hosts, in which the duration of data storage and the reward for each valid or invalid proof must be declared. In addition, maximum number of accepted invalid proofs will be mentioned. At the core of each contract, there is a Merkle root [38] of each file utilized to provide frequent proofs by the hosts.

Sia runs on its own open source blockchain and uses SiaCoin (SC) as its native cryptocurrency. However, Sia's developers are working on making it possible to use other cryptocurrencies on the network.

3.3 FILECOIN

FileCoin represents another decentralized storage network. It runs on top of IPFS. The InterPlanetary File System (IPFS) [42] was created to connect all computing devices in a distributed peer-to-peer file system, in order to avoid a single point of failure in the network. With the help of FileCoin, clients can store data on space offered by storage providers who are not their trusted parties [36]. Like other decentralized storage networks, clients need to be assured that their data are safe throughout time. To fulfill this demand two methods are proposed by FileCoin:

- *Proof-of-Spacetime*: Through this method, clients will be assured that during a specific period of time their data is being stored.
- *Proof-of-Replication*: Proof-of-Replication shows that data are safe in its dedicated physical storage locations and not a single node in the network has duplicated files on their own hardware.

The token used in FileCoin transactions is Filecoin (FIL).

3.4 SWARM

For storing Ethereum's public record fully decentralized and redundant, Swarm platform was formed [37]. In Swarm, participants share bandwidth and storage, enabling Swarm to provide the necessary infrastructures for services such as data-streaming, database services and payment channels to name a few. In this platform, consensus is reached by stake-weighted delegated voting system (also called *liquid democracy*). In a liquid democracy participants with a bigger share of network assets, such as coins or tokens, have more influence when casting a vote. In fact, each node's voting power is proportional to their share of the network. In contrast to the proof-of-work mechanism where the miners are rewarded for their CPU power, in Swarm, nodes are rewarded through proof-of-participation, which is effectively their level of participation in voting and making proposals on the network.

Swarm consists of a three layer architecture:

- Swarm core: Responsible for creating and managing new projects and it is the layer of network components and smart contracts.
- Swarm services: The second layer which increases operational services and helps participants make their investments easier.
- Swarm apps: Front-End or Back-End applications that which do not have to be necessarily built by Swarm.

Table 3 shows a comparison between Storj and Sia the two most used systems today [43, 44].

Table 3. Storj vs. Sia

Blockchain	Status	Point of Failure	Blockchain	Price
Storj	Active	Single Point of failures on Storj bridges	ERC20 token	Fixed (decided by Storj labs)
Sia	Active	Not a single point of failure (fully decentralized)	Sia Blockchain	Not fixed (has a market place)

3.5 THE RESEARCH CONTEXT

P.J. Taylor et al [45] have analyzed a number of existing blockchain-based studies. They observed that in this field, data storage and sharing is the second most researched topic after IoT, with 16% of all researches done in this area [based on Figure 6]. This shows IoT and data storage are the most trending topics in blockchain technology. They briefly concluded the aim of both public and private blockchains are solving these two main problems: single point of failure and data tampering.

Blockchain-based storage networks are proposed to store data in a more secure and available manner comparing to centralized storage systems. The stored content might be personal information of users, users' data or general information of a system. Some proposed ideas for improvement of existing blockchain-based storage networks as well as using blockchain technology to improve existing centralized systems are discussed below:

Root servers of Domain Name System (DNS) are located in only 13 different locations and various type of attacks (such as distributed denial of service attacks) can interfere with their functionality. Interruption of a single root can put a country in a state of confusion. In order to overcome this issue a new blockchain-based decentralization Domain Name System (DNS) is proposed in [46], which can prevent data-tampering by storing hash file of a domain name resolution zone file data. Also this system has multiple parallel parsing node, which prevent the system from collapsing in case of a single node failure.

S. Ali et al have designed a distributed data storage and access framework for PingER (Ping End-to-end Reporting). Their framework is based on a private blockchain where metadata of each file is stored there and also there are some Distributed Hash Tables (DHT) in different locations so as to store actual files off-chain. The aim of designing a worldwide end-to-end Internet performance measurement framework is removing the centralized party [47].

To overcome the search ability in storage blockchains, a system with keyword search service is presented in [48]. In this proposed system, all data and specified keywords will be encrypted before transmitting on the network just like other blockchain networks and data would be sent to the blockchain nodes (storage providers) to be stored. Although keywords are kept on blockchain itself, data providers would grant permissions to the other nodes on the network. As a result data owner and permissioned nodes can search for the data on the blockchain.

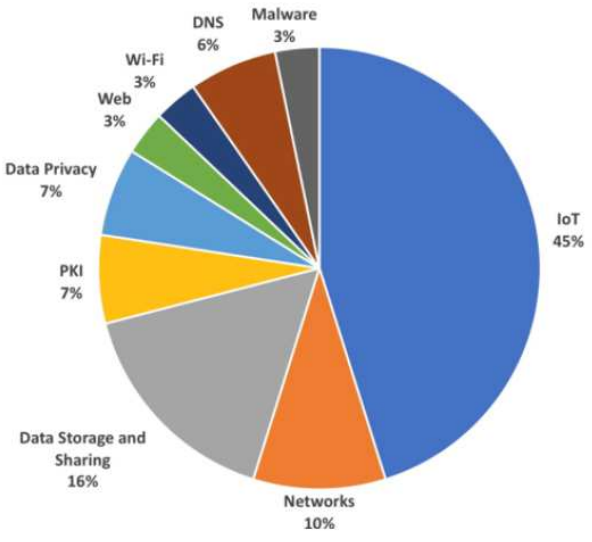

Figure 6 - Chart of Research Area's on Blockchain [45]

In order to prevent data fraud, Ramachandran et al have proposed a system. In this system a meta-data that consists of data origin, data owner and transformations done on the data should be recorded. This package is called Data Provenance. It is believed as long as the majority of this network are honest, malicious modification on data can be prevented [49].

One of the proposed solution to the problem of data privacy of traditional cloud storage systems is attribute-based encryption (ABE). However, there's a blind spot in this solution: the data encryption ability by private key generator itself. Nevertheless, the threat of a single point of failure exists is traditional cloud storage systems merely due to their centralized nature. In [50] a blockchain-based framework with fine-grained access control in decentralized storage systems is offered. This model uses the

combination of the decentralized storage system interplanetary file system, the Ethereum blockchain, and ABE technology. In this platform, data owner can specify the access policy for other nodes and also keyword search on encrypted data is implemented.

Intelligent agents in the field of Artificial Intelligent (AI) are defined as devices that comprehend the environment and take actions that increase the chance of success of their predefined targets. AI systems use a database to make better decisions. K. Salah et al have proposed a blockchain for AI [51]. This blockchain by providing a decentralized storage space that maintenances data and keeps it safe from being tampered or manipulated, provides conditions for proper decision making.

BlockHouse [52] is a private blockchain aiming to create a storage system. Just like other blockchain-based storage networks, members rent out their unused hardware space but within the private blockchain. Data availability and redundancy are checked in fixed time intervals. This network has a dual smart contract for logging, payment and securing the storage process. Proof of Retrievability (PoR) is the consensus algorithm used in this project. BlockHouse is created in order to store critical data of small or medium enterprises within the network instead of storing on a remote cloud.

Karunakaran et al [53] studied storage system for companies, which have their data distributed across the organization. They believe need of data extraction in such systems might cause a disaster. They offered a decentralized data storage method with the help of blockchain and artificial intelligent. In their proposed system, blockchain handles data protection whilst it is a cheaper solution, and AI would take care of data understanding, knowledge creation and also retrievability.

Internet of Things (IoT) is growing daily and produced data of this technology are increased respectively. This massive amount of important data is stored on third parties storage spaces that assigns trust issues to the third parties. To overcome this problem, [54] offers implementing a blockchain-based multi-center storage system as well as encryption, consensus algorithms and smart contract to solve the trust issue and ensure the security of the data.

4 ADVANTAGES OF DECENTRALIZED STORAGE

Decentralized storage networks have built in order to resolve the aforementioned issues in centralized storage systems and to bring more advantages to the world of technology. Some of the advantages of using blockchain-based storage systems are explained in the following.

4.1 PRIVACY

Earlier we learned that blockchain uses a different privacy model comparing to server-based services. Each person can create their own Blockchain identity without needing the help of any central party which makes this identity completely

disconnected from their real life identity. Thus account management is done anonymously and the identity of the user is concealed, therefore providing a higher degree of privacy. Unlike traditional systems that a person should register their personal information (such as full name and bank account information) in the network, a person's true identity cannot be revealed on the blockchain unless they give up their private key. Also, storage fees are paid by cryptocurrencies with the help of a digital wallet [10, 11].

As discussed, one of the most significant technologies for solving privacy problems in cloud storage systems is attribute-based encryption (ABE), which would allow private key generator to access all the data. Blockchain systems could solve the same problem by providing the users the ability to generate and distribute secret keys [50].

4.2 SECURITY

All data must be encrypted before being transmitted on the blockchain. This means only people with access to the decryption key can access the contents of a file. Even though some centralized storage networks also offer encryption, since the files on a decentralized blockchain are divided into smaller shards (fractions) and the shards are distributed among different storage providers, we can be confident that even a malicious node cannot decrypt a file wholly and access its data unlike cloud-based storage systems. This means no person, organization or party can process existing data in a network. Moreover, since each shard is stored on at least three locations, the data will always be accessible even if some nodes are unavailable or are facing hardware failures. Even if some fractions are lacking, a file can be recovered with the help of erasure coding. In addition, storage providers are required to prove that the data has not been manipulated. Even in case of manipulation, the altered part can be easily accessed with the help of the file's Merkle root [38]. The centralized storage systems, however, neither assure their clients about the integrity of their data, nor do they reveal the ways in which their data would be processed [35-37, 4, 40].

For example, a blockchain-based auditable and distributed access control layer can be enabled on top of storage network. It is a useful method for storing IoT data and by this approach the potential of all isolated data silos can be extracted while users are empowered with data ownership instead of centralized parties [19].

4.3 BANDWIDTH AND COST

In cloud storage scenario, when a user needs to download a file, the whole file would be downloaded from one of the servers of the service provider. Although, some of service providers claim that download would be occurred from the best available server of the moment, still it has to be done through a single connection. But in case of a file requirement from blockchain-based networks, the file must be retrieved from the network. It means each fraction has to be downloaded from a different storage provider. In that case, downloads would be run in parallel which can increase the

available bandwidth to its maximum and reduce the download time to its minimum [35]. For network standardization and assurance of its efficiency, Storj has defined some prerequisites. Every storage node operator should meet certain requirements such as minimum unmetered available bandwidth, minimum up/downstream bandwidth and etc., in order to join the network [55].

In traditional storage systems, a specific fee needed to be paid in advance for a package (for example 5$/month for 5T of storage space) and clients usually pay for more storage space than what they actually need. But in blockchain storage systems, costs would be calculated based on each user's usage and it is paid during the use and not earlier [56].

Moreover, blockchain-based storage systems are generally cheaper than traditional storage systems. They also allows the users to choose their preferred hardware type of storage between available options as well as the duration of their usage [40]. Blockchain storage comes in at about $2/terabyte/month according to [57], which is much lower than Amazon S3.

4.4 REPUTATION SYSTEM

Blockchain-based data storage systems also use a mechanism called *the reputation system*. As it is defined in [58], reputation is a mechanism to measure how much the community trusts a node, based on their previous transactions and interactions. The greater the node's reputation, the more trustworthy it is on the network. Since in such networks most of transactions happen between parties that don't know each other, it is important for the users to determine whether to interact with a specific node in the future transactions or not [59]. This features allows the network to automatically validate space providers' sincerity to make sure the hosts live up to their claims and if not are removed from the network. The greatest feature of the reputation system is that it allows clients to rate their experience, incentivizing storage providers to be trustworthy. In other words a storage system like Storj is not reliant only on users' opinions. This means the malicious nodes will be eventually dropped out of the network [4, 35, 37].

5 OPEN CHALLENGES AND FUTURE REASEARCH

It is clear that this immature technology is still struggling with many challenges and as a result lots of improvements are yet to occur. In this section the common issues of individuals or organizations toward blockchain-based storage are discussed.

5.1 SECURITY

Although we mentioned security is one of the prominent features of blockchain networks comparing to centralized systems, it should also be noted that necessarily

blockchain systems are not one hundred percent secure. In other words, risk of arising security issues are remarkably lower comparing to centralized networks, but not completely vanished. In addition, in need of data editing or sharing with a third party since the files must be encrypted and decrypted every time, security issues may increase. Put it differently, data is secure on storage, not transmitting on the network.

Also there are some attacks that can threaten the blockchain itself and consequently the running application on it. 51% attack is a well-known existing attack that can happen in blockchains which use Proof of Work (PoW) consensus algorithm. In such blockchains a group of nodes that holds more than 51% of all the computation power of the blockchain can control the network and cause to occur other attacks such as selfish mining and double spending. To prevent 51% attack, a blockchain must be containing a massive number of nodes so that no group would be able to control the network in their favor [11, 60, 61].

Selfish mining happens when a dishonest node finds the nonce sooner than other miners but keep it to themselves and mine until they are ahead of the proofed chain [60]. Then they reveal their own private chain and gain the prize whereas their offered chain is the longest. To overcome selfish mining, [62] offers freshness mechanism. In this method nodes should be accepting the most newly validated block or the first received block, in case of two blocks having the same amount of validation.

When a node spends the same amount of cryptocurrency in more than one transaction, double spending happens. Listening Period technique or waiting to receive more confirmation on each block are proposed to solve this issue [60].

5.2 LACK OF DATA-BASED DECISION MAKING

A huge number of companies and organizations consider their collected data a significant resource which can be analyzed and processed in order to help them make data-based decisions. This process cannot be accomplished in blockchain-based storage systems because all data are encrypted before being stored by storage providers. However, companies can build their own blockchain-based storage system, such as offered in BlockHouse, and give the permission and required keys to their certified agents. In this case agents can extract all the data from the chain and analyze it to meet companies' needs.

Also data encryption is not required in all private blockchains where all of the members are accredit. In this scenario, blockchain storage system can be used as a proof-tampered and trackable solution for data storage.

5.3 LACK OF LEGAL CONSTRAINTS

Smart contracts are set between two parties and some vital information and conditions are written in them which makes it hard for both parties to deny or violate their agreement. However, in the case of fraud, scam or any unexpected issue there is no legal reference or court of law to stand.

5.4 SCALABILITY ISSUES

It sounds easy in words to grow a blockchain network by accepting any new volunteer node in it. But in fact maintaining the network efficiency and security as it grows, is not easily acquired. Scalability is a common challenge in blockchain networks why it can cause problems such as long delays.

Joancomartí et al have studied Bitcoin blockchain scalability issues and offered some solution for it. They claimed that possible delays is not the only problem. *Bootstrap time* is the time it takes a new node to join the network, download and analyze the history of the network, which for an old huge blockchain like Bitcoin can be quite expensive and time taking. Also they studied following solutions for scalability of the network: 1. to decrease the volume of necessary information in each transaction so as to jamming more transactions in a block, 2. changing the block size to finding the optimum size [63].

In general, scalability issues of blockchain can be divided to 3 main groups: Throughput, cost and capacity. Capacity is the size of all previously performed transactions that miner should store. This volume is increasing daily. Even small transactions need to pay the transaction fee. This can turn into a problem, when size of transactions and subsequently their fee is too small, but a massive number of them should be transmitted on the network. And finally, the throughput issue occurs when transactions are waiting to be a part of a block. Due to limitation of the block size, this time can be so long [64].

5.5 ACESS CONTROL

Although record of previous transactions would always be accessible in blockchain and huge amount of data must be replicated on each single node, blockchain should not be considered a database itself. These two main specifications of blockchain could cause bloating if huge files were stored on blockchain. Regarding this issue huge files shall be stored off-chain, as we deeply discussed about them in this survey. But blockchain storage networks do not allow file sharing between users. To overcome this issue [65] has offered a smart contract based solution, however it only solve the problem in IPFS.

5.6 REPUTATION SYSTEM ISSUES

In [66] trust in virtual communities such as Facebook or Twitter is discussed. It highlights the fact, though in global reputation systems we can see recommendations' result of the other agents, we have to keep in mind, that result has originated from all nodes' opinion and it might not be a reliable outcome, while the other components themselves may not be trustworthy to us. To solve this issue, they offer a *local reputation* system, in which only the result of recommendations' of the entourage of the user would be taken to account. This idea can be implemented in blockchain systems so as to empower us to utilize only the recommendations from the people we do trust in.

5.7 SWITCHING TO BLOCKCHAIN

Blockchain storage networks are a brand new technology which may look temping at first sight. However, switching to a blockchain network is not necessarily the best solution for any individual or company. Pros and cons of blockchain systems must be fully studied before switching on them.

All in all, for a single person it is a cheaper solution to store data which is secure enough. Nevertheless, companies and organizations must be more cautious in this regard, as it does not support cloud storage existing solutions such as data analysis or processing so far.

5.8 OPEN QUESTIONS

Each blockchain or system is formed to reach a specific goal. Each demand or necessity to overcome existing challenges of each era or even novel ideas, can be the causative agents of future changes. In this section, some ideas regarding blockchain based storage systems improvement are considered:

In future, the debated technology can be also applied to private or consortium blockchains, which will enable the members of those blockchains (e.g. various organizations) to use the collective space of the blockchains, instead of using limited space of personal computers, incur excessive costs of purchasing storage hardware or taking the risk of having their files uploaded on an external system.

Some blockchains can be formed to overcome a specific feature, for instance focusing only on speed of downloading stored files. To create such facility, storage space of each host should meet specific standards. For storing high value data, they can be only stored on nodes with high availability or having more redundancy than usual files.

Quantum computing can also be merged in many different fields of this technology. From secret key exchange and secret sharing to authentication [67]. Furthermore, instead of sharding method in now existing blockchains, with the help of quantum entanglement a group of particles can be generated. The most important specification of quantum entanglement is that no particle can be described alone, and the whole batch together would determine state of each other.

Cloud service providers also can move on to this technology where a chain hold by all members of that network could keep the track of all transactions. All information is encrypted before transmitting on the network, in fixed time intervals proofs are sent to users, cost is calculated based on the usage thereupon it is cheaper than previous model.

6 CONCLUSION

Blockchain is a disruptive technology that with its peer to peer and decentralized features can make changes in a wide variety of industries. Storing and retrieving data

in cloud storage is one of the crucial and controversial issues of this era. Blockchain based storage systems can overcome many issues and shortcoming of traditional storage systems. In this survey a new approach to data storage with the aim of increasing privacy and security is discussed.

However, challenges and problems in this area such as scalability issues, data analyzing and accessing are still debatable, it is believed that blockchain-based storage, like any other newborn application of this technology, is still in progress to reach its maturity.

It is good to have in mind that each consensus protocol has formed to act in a blockchain with certain targets e.g. speed. Protocols can be merged, altered or even be created from the beginning to meet different goals. For a deeper investigation in this area we plan, so as to reach an improved algorithm for proof-of-storage in Storj.

References

1. Zeng, W., Zhao, Y., Ou, K., Song, W.: Research on Cloud Storage Architecture and Key Technologies. Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human. pp. 1044-1048. ACM, Seoul (2009). doi: 10.1145/1655925.1656114
2. Mogarala, A.G., Mohan, K. G.: Security and Privacy Designs Based Data Encryption in Cloud Storage and Challenges: A Review. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-7. IEEE, Bangalore (2018). doi: 10.1109/ICCCNT.2018.8493674
3. Charanya, R., Aramudhan, M.: Survey on Access Control Issues in Cloud Computing. 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), pp. 1-4. IEEE, Pudukkottai (2016). doi: 10.1109/ICETETS.2016.7603014
4. Wilkinson, S., Boshevski, T. Brandoff, J., Buterin, V.: Storj: A Peer-to-Peer Cloud Storage Network, vol. 1.01 (2014). https://storj.io/storj2014.pdf (last access 24-Apr-2019)
5. Androutsellis-Theotokis, S., Spinellis, D.: A survey of peer-to-peer content distribution technologies. ACM Computing Surveys (CSUR) 36(4), 335-371 (2004). doi: 10.1145/1041680.1041681
6. Hasan, R., Anwar, Z., Yurcik, W., Brumbaugh, L., Campbell, R.: A Survey of Peer-to-Peer Storage Techniques for Distributed File Systems. International Conference on Information Technology: Coding and Computing (ITCC'05), pp. 205-213. Vol. 2. IEEE, Las Vegas, NV (2005). doi: 10.1109/ITCC.2005.42
7. Schvachko, K., Kuang, H., Radia, S., Chansler, R.: The Hadoop Distributed File System. 2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST), pp. 1-10. IEEE, Incline Village, NV (2010). doi: 10.1109/MSST.2010.5496972
8. Chang, F., Dean, J., Ghemawat, S., Hsieh, C.W., Wallach, A.D., Burrows, K., Chandra, T., Fikes, A., Gruber, E. A.: Bigtable: A Distributed Storage System for Structured Data. ACM Transactions on Computer Systems (TOCS), pp. 1-26, Vol. 26, no. 2. ACM, NY, USA (2008). doi: 10.1145/1365815.1365816
9. Blomer, J.: A survey on Distributed File System Technology. Journal of Physics: Conference Series 608:012039 (2015). doi: 10.1088/1742-6596/608/1/012039
10. Nakamato, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

11. Zheng, Z., Dai, H., Xie, S.: Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services 14(4), 352-375 (2018). doi: 10.1504/IJWGS.2018.10016848
12. Sankar, L.S., Sindhu, M., Sethumadhavan, M.: Survey of consensus protocols on blockchain applications. 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1-5. IEEE, Coimbatore (2017). doi: 10.1109/ICACCS.2017.8014672
13. Wahab, A., Memood, W.: Survey of Consensus Protocols. Computing Research Repository (CoRR) (2018).
14. Nguyen, G.T., Kim, K.: A Survey about Consensus Algorithms Used in Blockchain. Journal of Information Processing Systems. pp. 101-128, Vol. 14, no. 1 (2018). doi: 10.3745/JIPS.01.0024
15. Buterin, V.: Ethereum: A Next Generation Smart Contract and Decentralized Application Platform (2014). https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a next generation smart contract and decentralized application platform-vitalik-buterin.pdf (last access 24-Apr-2019)
16. Mettler, M.: Blockchain Technology in Healthcare: The Revolution Starts Here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-3. IEEE, Munich (2016). doi: 10.1109/HealthCom.2016.7749510
17. Vaughan,W., Bukowski, J., Rempe, G.: Tierion Network: A Global Platfrom for Verifiable Data (2017).
18. Dorri, A., Kanhere, S. S., Jurdak, R., Gauravaram, P.: Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618-623. IEEE, Kona, HI (2017). doi: 10.1109/PERCOMW.2017.7917634
19. Shafagh, H., Hithnawi, A., Burkhalter, L., Duquennoy, S.: Towards Blockchain-based Auditable Storage and Sharing of IoT Data. Proceedings of the 2017 on Cloud Computing Security Workshop, pp. 45-50. ACM, Dallas, Texas (2017).
20. A Blockchain-Based Decentralized Reputation System. https://www.drep.org/ (last access 24-Apr-2019)
21. Abeyrante, S. A., Monfared, R. P.: Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger. International Journal of Research in Engineering and Technology, 05(09), 1-10 (2016). doi: 10.15623/ijret.2016.0509001
22. Ambrosus: A Blockchain-Based Ecosystem for Supply Chains. https://ambrosus.com/assets/en/-White-Paper-V8-1.pdf (last access 24-Apr-2019)
23. Rakic, B., Levak, T., Drev, Z., Savic, S., Veljkovic, A.: OriginTrail: First Purpose Built Protocol for Supply Chains Based on Blockchain (2017). https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf (last access 24-Apr-2019)
24. Vechain. https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper_en_v1.0.pdf (last access 24-Apr-2019)
25. Hess, Z., Malahov, Y., Pettersson, J.: Aeternity blockchain: The Trustless, Decentralized and Purely Functional Oracle Machine (2017). https://www.aeternity.com/aeternity-blockchain-whitepaper.pdf (last access 24-Apr-2019)
26. Peterson, J., Krug, J., Zoltu, M., Williams, A. K., Alexander, S.: Augur: a Decentralized Oracle and Prediction Market Platform (2018). https://www.augur.net/whitepaper.pdf (last access 24-Apr-2019)

27. IRide: Ridesharing Powered by Ethereum Blockchain. https://iride.io/whitepaper/iRide-whitepaper.pdf (last access 24-Apr-2019)
28. Ernest, A. K.: The Key to Unlocking the Black Box: Why the World Needs a Transparent Voting DAC (2014). https://followmyvote.com/wp-content/uploads/2014/08/The-Key-To-Unlocking-The-Black-Box-Follow-My-Vote.pdf (last access 24-Apr-2019)
29. BitGive Foundation. https://www.bitgivefoundation.org (last access 24-Apr-2019)
30. One + One. https://1p1.io/uploads/documents/One+One-Whitepaper-EN.pdf (last access 24-Apr-2019)
31. Ericson, P., Harris, P., Larcombe, C., Pekari, T., Snook, K., Dubber, A.: MTFLabs: Blockchain (2016). http://musictechfest.net (last access 24-Apr-2019)
32. Grid+. https://gridplus.io (last access 24-Apr-2019)
33. OpenBazaar. https://openbazaar.org (last access 24-Apr-2019)
34. YouToken: Blokchain Crowdfunding Platform. https://www.youtoken.io/ (last access 24-Apr-2019)
35. Vorick, D. Champine, L.: Sia: Simple Decentralized Storage (2014). https://sia.tech/sia.pdf (last access 24-Apr-2019)
36. FileCoin: A Decentralized Storage Network. https://filecoin.io/ (last access 24-Apr-2019)
37. Swarm Fund: The Blockchain for Private Equity. https://swarm.fund/whitepaper (last access 24-Apr-2019)
38. Merkle, R. C.: Protocols for Public Key Cryptosystems. 1980 IEEE Symposium on Security and Privacy, pp. 122-134. IEEE, Oakland, CA (1980). doi: 10.1109/SP.1980.10006
39. Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E.: Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab. Lecture Notes in Computer Science, pp 79–94 (2016). doi:10.1007/978-3-662-53357-4_6
40. Wilkinson, S., Lowry, J.: Metadisk: Blockchain-Based Decentralized File Storage Application (2014). https://storj.io/metadisk.pdf (last access 24-Apr-2019)
41. Storj V3: A Decentralized Cloud Storage Network Framework (2018). https://storj.io/white-paper/ (last access 24-Apr-2019)
42. Benet, J.: IPFS - Content Addressed, Versioned, P2P File System (2018). https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf (last access 24-Apr-2019)
43. https://www.reddit.com/r/storj/comments/6efd8c/sia_vs_storj/ (last access 24-Apr-2019)
44. https://delegatecall.com/questions/whats-the-difference-between-filecoin-siacoin-and-storj-9bc520bb-37d1-4dc0-85e2-878de05a07d9 (last access 24-Apr-2019)
45. Taylor, P. J, Dargahi, T., Dehghantanha, A., Parizi, R. M., Choo, K. R.: A Systematic Literature Review of Blockchain Cyber Security. Digital Communications and Networks (2019). doi: https://doi.org/10.1016/j.dcan.2019.01.005
46. Liu, J., Li, B., Chen, L., Hou, M., Xiang, F., Wang, P.: A Data Storage Method Based on Blockchain for Decentralization DNS. 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, pp. 189-196 (2018). doi: 10.1109/DSC.2018.00035
47. Ali, S., Wang, G., White, B., Cottrell, R. L.: A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, pp. 1303-1308 (2018). doi: 10.1109/TrustCom/BigDataSE.2018.00179

48. Do, H. G., Ng, W. K.: Blockchain-Based System for Secure Data Storage with Private Keyword Search. 2017 IEEE World Congress on Services (SERVICES), Honolulu, HI, pp. 90-93 (2017). doi: 10.1109/SERVICES.2017.23
49. Ramachandran, A., Kantarcioglu, M.: SmartProvenance: A Distributed, Blockchain Based Data Provenance System. Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, Tempe, AZ, USA, pp. 35-42 (2018). doi: 10.1145/3176258.3176333
50. Wang, S., Zhang, Y., Zhang, Y.: 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
51. Salah, K., Rehman, M. H. U., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: Review and Open Research Challenges. IEEE Access, vol. 7, pp. 10127-10149 (2019). doi: 10.1109/ACCESS.2018.2890507
52. Perard, D., Gicquel, L., Lacan, J.: BlockHouse: Blockchain-based Distributed Storehouse System. 9TH Latin-American Symposium on Dependable Computing, arXiv: 2001.07016v1 (2019).
53. Karunakaran, A., Divakaran, P.: Decentralized Block Chain Data Storage Using Artificial Intelligence. Our Heritage, GRCF Dubai International Conference on "Sustainability and Innovation in Higher Education, Engineering Technology, Science, Management and Humanities", Vol. 67, No.9, pp 8-13 (2019).
54. An, Y., Liu, Y., Zeng, J., Du, H., Zhang, J., Zhao, J.: Trusted collection, management and sharing of data based on blockchain and IoT devices. 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China, pp. 27-32 (2019). doi: 10.1109/SOLI48380.2019.8955019
55. https://documentation.storj.io/before-you-begin/prerequisites (last access 29-Jan-2020)
56. https://medium.com/coinmonks/differences-between-ppio-filecoin-storj-20cdf7b3b02e (last access 14-Jun-2019)
57. http://techgenix.com/blockchain-technology-for-cloud-storage/ (last access 14-Jun-2019)
58. Dennis, R., Owen, G.: Rep on the block: A next generation reputation system based on the blockchain. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp 131-138 (2015). doi:10.1109/icitst.2015.7412073
59. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision Support Systems, Vol. 43 no. 2, pp 618–644 (2007). doi:10.1016/j.dss.2005.05.019
60. Huynh, T. T., Nguyen, T. D., Tan, H.: A Survey on Security and Privacy Issues of Blockchain Technology. 2019 International Conference on System Science and Engineering (ICSSE), Dong Hoi, Vietnam, pp. 362-367 (2019). doi: 10.1109/ICSSE.2019.8823094
61. Conti, M., Kumar, S., Lal, C., Ruj, S.: A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, Vol. 20, no. 4, pp. 3416-3452 (2018). doi: 10.1109/COMST.2018.2842460
62. Heilman, E.: One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, a Solution for the Honest Miner. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, pp. 161-162 (2014).
63. Herrera-Joancomartí J., Pérez-Solà C.: Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions. Modeling Decisions for Artificial Intelligence, MDAI 2016, Lecture Notes in Computer Science Vol. 9880, pp. 26-44 (2016). doi: 10.1007/978-3-319-45656-0_3

64. Chauhan, A., Malviya, O. P., Verma, M., Mor, T. S.: Blockchain and Scalability. 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, pp. 122-128 (2018). doi: 10.1109/QRS-C.2018.00034
65. Steichen, M., Norvill, R., F., Shbair, W., State, R.: Blockchain-Based, Decentralized Access Control for IPFS. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, pp. 1499-1506 (2018). doi: 10.1109/Cybermatics_2018.2018.00253
66. Fotia, L., Messina, F., Rosaci, D., Sarné, G. M. L.: Using Local Trust for Forming Cohesive Social Structures in Virtual Communities. The Computer Journal, Vol. 60 no.11, pp 1717–1727 (2017). doi:10.1093/comjnl/bxx072
67. Karlsson, A., Koashi, M., Imoto, N.: Quantum Entanglement for Secret Sharing and Secret Splitting. The American Physical Society, Physical Review A, vol. 59, no. 1, pp 162-168 (1999). doi: https://doi.org/10.1103/PhysRevA.59.162

Mehdi Aminian received his B.Sc. degree in computer engineering from the Tehran University, Tehran, Iran, in 2003, and his M.Sc. and Ph.D. form Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in the field of Computer Engineering in 2005 and 2012, respectively. He is currently a faculty member in the Department of Electrical and Computer Engineering, Islamic Azad University–North Tehran Branch, Tehran, Iran. His research interests are Blockchain Technology, Internet of Things, Fog Computing and SDN Networks.

Nazanin Zahed is the master student of Computer Networks in Islamic Azad University – North Tehran Branch. She received her bachelor degree in Information Technology Engineering also from IAU-TNB in 2015. Her research interests are Blockchain Technology, Distributed Systems and Storage Networks.

Bahman Javadi is an Associate Professor in Networking and Cloud Computing at Western Sydney University. Before that he appointed as a Research Fellow at the University of Melbourne, Australia. He was a Postdoctoral Fellow at the INRIA Rhone-Alpes, France in 2008–2010. He received his MS and PhD degrees in Computer Engineering from the Amirkabir University of Technology in 2001 and 2007, respectively. His research interests are Cloud Computing, Edge Computing, Reliability, Internet of Things and Smart Computing.