JOURNAL OF DECISION MAKING AND HEALTHCARE
Volume 2 (2025), No. 3, 185–191
https://doi.org/10.69829/jdmh-025-0203-ta02
Tulipa Opera Scholarum

DECENTRALIZED CLOUD COMPUTING USING BLOCKCHAIN

DARSHAN MANOJ[1], DANIEL PAIVA[2], AND GAUTAM SRIVASTAVA[2,*]

[1] *Thomas Lord Department of Computer Science, University of Southern California, Los Angeles, USA*
[2] *Brandon University, Brandon, Canada*

Abstract. Cloud Computing is an on-demand model that provides and allows various digital resources to be accessed over the internet. With its rise to prominence, cloud computing has allowed the digital world to become more convenient, flexible, and cost effective, thus making it a tempting alternative in comparison to deploying and maintaining the servers required to meet the same needs. An abundant amount of data is constantly being processed, stored, and managed through the cloud and with this data comes the concern of data security and integrity. In this paper we examine the different data issues facing a cloud environment and discuss a decentralized model using the blockchain framework. Blockchain is a shared public ledger that grows accordingly to its confirmed transactions and has become notorious over the past decade for its use of cryptocurrency as well as its key characteristics of decentralization and data transparency. With these concepts of blockchain we can provide a more secure and reliable cloud environment.

Keywords. Blockchain, Cloud Computing, Decentralized, Storage Systems, Security.

1. Introduction

1.1. Cloud computing.

Cloud Computing involves the various services such as data storage and computing power made readily available over the internet [9–12]. In comparison to maintaining the infrastructure required to operate a required service, cloud computing provides a convenient alternative method of just accessing the resources via an internet connection [3]. In turn, companies that host these cloud services can assign fixed rates or prices that users of the cloud can then pay to access the amount they use. Both the users and the cloud providers can then benefit from this arrangement since the amount of resources being used can be determined and thus no resources are being wasted than what is needed. Typical examples of cloud computing involve email services such as Gmail and data backups for a smartphone such as iCloud.

Within any cloud service, several service models [4] can be defined:

- Infrastructure as a Service: Hardware and software that can be rented and used for servers, storage, and networking. Considered as the building block of cloud computing.
- Platform as a Service: Tools and software required to build applications that may involve database management, operating systems, and other development.
- Software as a Service: Applications delivered to the user over the internet without providing the underlying hardware or software needed to operate the application.

Similarly, several cloud models are also defined in order to meet different solutions:

- Public Cloud: Computing power shared to the public where users can access large amounts of resources via the internet with the benefit of being able to rapidly scale a service. Typically used for services that demand various amounts of resources.

*Corresponding author.
E-mail address: dmanoj@usc.edu (D. Manoj), paivadf69@brandonu.ca (D. Paiva), srivastavag@brandonu.ca (G. Srivastava)
Accepted: August 09, 2025.

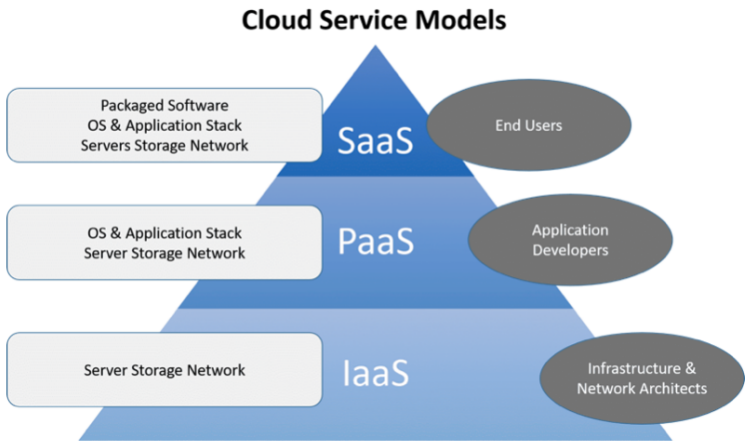

FIGURE 1. Cloud Service Model Hierarchy

- Private Cloud: Exclusive to specific users and operates behind a corporate firewall where data is managed and controlled at a discrete level typically for a specific purpose.
- Hybrid Cloud: Combination of more than one cloud such as public and private cloud where both its respective services are integrated into one making it ideal for scalability.
- Community Cloud: Infrastructure managed by several providers but belongs to a specific community. Ideal for managing projects that are shared amongst various individuals.

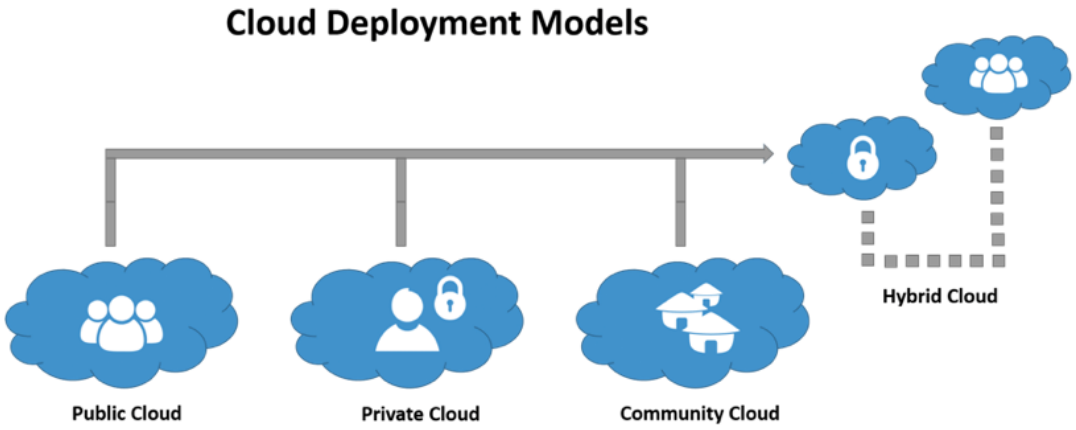

FIGURE 2. Cloud Deployment Models

1.2. **Blockchain.** Blockchain is a dynamic list of digital blocks that are stored and linked together onto a public database using cryptography. Since the blockchain can be accessed and viewed by the public and is not owned by any central authority, the blockchain can be referred to as a shared public ledger [2]. These blocks will contain the following:

- Time Stamp: Indicating when the block was generated.
- Main Data: Depending on the application this can vary, but a common example would be a bitcoin transaction with a digital signature that will ensure the user's privacy.
- Hash Value: When a block is being added it is assigned a hash value from a cryptographic algorithm as well as the hash values that point to the block before and after it.

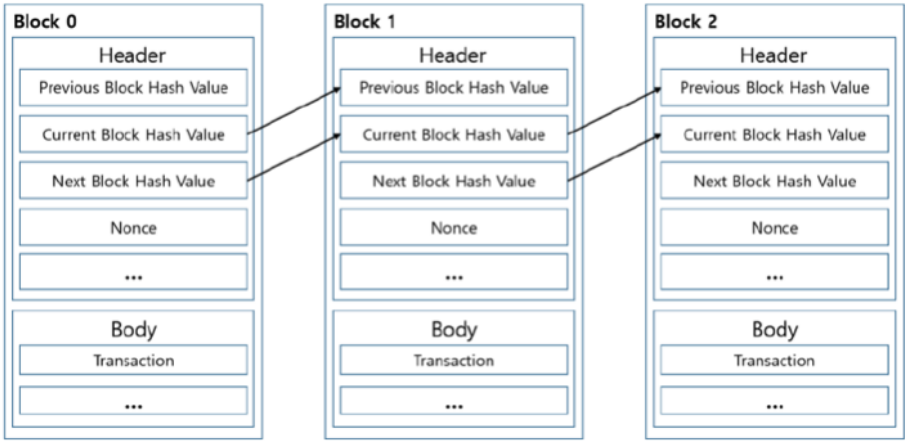

FIGURE 3. Blockchain Architecture

Every blockchain's foundation relies heavily on its three properties of decentralization, transparency and immutability. A blockchain does not store its information in a single location unlike a centralized server that would store and administer information at a single point. Centralization follows a client-server model in which queries are being sent to a server for data requests and that data is then sent back to whoever made a request. With a centralized model you are susceptible to attacks as well as any crashes or shutdowns. If delicate information is being managed on your server then this can become a concern when data becomes corrupted or stolen. With a decentralized model we can alleviate this issue because the information is distributed across many nodes. These nodes are connected to each other through a peer-to-peer network and everyone has equal claim to data, thus if one node were to be attacked then it would not affect the overall state of the data [14]. In addition, a decentralized model can also be more beneficial for speed as you are able to access data from various nodes within a peer-to-peer network rather than a single node in the centralized model [15].

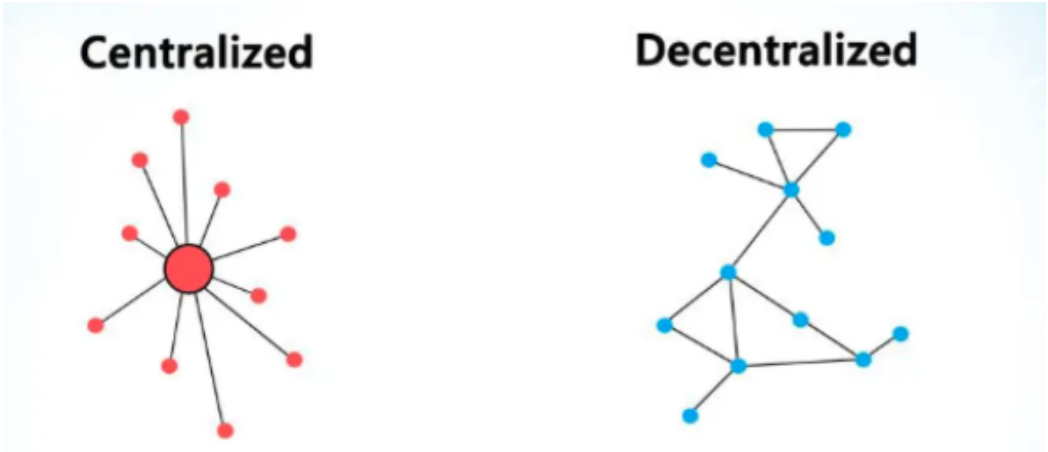

FIGURE 4. Centralized VS Decentralized Model

Blockchains are classified as being transparent, meaning that the chain is public and can be viewed by anyone while still maintaining the security and privacy of the nodes in the network. Although a person may still be able to view all the transactions, they would not be able to access a block's personal information since a block is assigned a hash value from a cryptographic algorithm. This adds a level of

accountability that cannot be obtained through a centralized model. Immutability is another significant property that allows a blockchain to be tamper-proof meaning that anything that is entered into the chain cannot be altered with. If any change were to be made, then it would be reflected in a block's hash value when it is validated by other previous blocks in the chain.

1.3. **History and uses.** Blockchain was first introduced through a cryptocurrency called bitcoin in 2008 through a paper published by Satoshi Nakamoto. Bitcoin is a digital currency that manages transactions of the market where tokens are either bought or sold and then recorded onto the blockchain [1]. Software known as bitcoin wallets relies on the blockchain to determine the balance of a user and whether they can spend tokens. When a transaction is first initiated it becomes available to everyone on the network so that it can be verified [7]. Any computer on the network can opt in and decide to compute a complex mathematical hash to confirm that the requested transaction has a valid hash value which then can be added to the blockchain. Those who are involved in verifying the transactions are called miners.

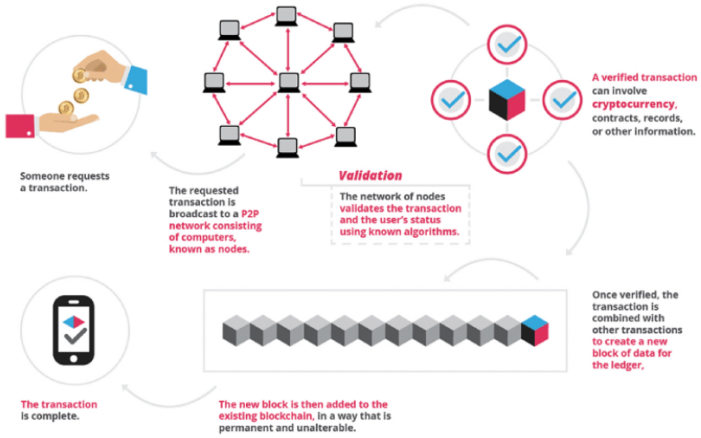

FIGURE 5. Transaction Process within a Blockchain

Miners are constantly trying to produce a hash value that is equal or below to the target hash they are solving for. The chances of determining such a value are extremely low, especially when the difficulty level of a block is changed and determines how often a block can be added to the blockchain. Regardless, these miners are essential for validating previous transactions which help prevent any duplication or tampering. In return, these miners are compensated for their verifications and are rewarded with bitcoin if they verify a certain amount of transactions and are the first person in the network to validate those transactions. Any person who participates in the blockchain also receives a copy of the blockchain thus making it further difficult to tamper with a transaction because they would have to change every copy of the blockchain on the network.

2. Related Work

For a cloud environment to be implemented within a blockchain framework, the users of the cloud must be connected to each other via a peer-to-peer network to fulfill the blockchain's decentralized model [16]. A pre-existing decentralized cloud storage model called Storj involves data within the cloud such as files being stored, managed, and processed across the network meaning that everything that happens to the file would be entered into the blockchain [6]. Each user is responsible for encrypting their own file and controlling their respective encryption keys that grants them access to their files. That file is then broken up into chunks of data and is distributed throughout the network by duplicating

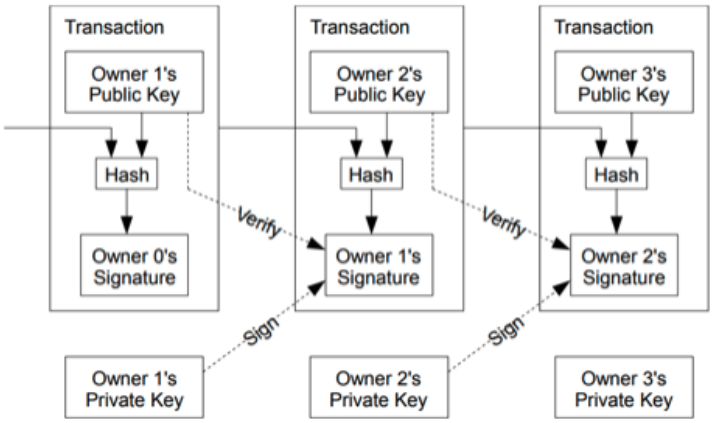

FIGURE 6. Example of Bitcoin Architecture

each chuck to ensure redundancy of the blockchain. Those chunks are split up randomly and hashed numerous times throughout the network. When the user is requesting access to their data, they go through a blockchain-based hash table where their entire file gets reconstructed from each individual chunk that is sent from each user in the network. An encryption key is then used by the person who requested that data and can be used to decrypt the file [5].

When users go to access their data, the chunks of their requested file are compared to make sure that they are identical and if something is different, that will indicate a manipulation of data which then results in the user with a different chunk being removed from the network. This ensures a more secure and stabilized cloud environment rather than a centralized cloud model. Suppose a piece of a file is decrypted and exposed to an intruder in the network: They would only have a partial file and wouldn't be able to identify who the file belongs to. More than one copy of that data is stored in multiple locations, so if one node were to fail a user could still access their file elsewhere. The more active nodes there are in the network, the faster a user can access their data in accordance to a decentralized framework.

An auditing process is also used for nodes holding contents of a file to ensure that they are holding onto the correct chunk. If they are holding onto the correct chunk of data that they are agreed to hold onto, they will be compensated for their storage much like how a bitcoin miner is compensated for their work on confirming the blockchain ledger. The main difference here is that the blockchain is being used as a storage facility where a user can access their chunks of their file from various users in the network. The basis of this framework revolves around the blockchain's key feature of decentralization, but on its own it is not ideal for a storage center, but rather a ledger of transactions. Thus, for this proposed framework to be a feasible alternative there must be an underlying layer where the storage of these files will occur, and the actions of those files be recorded onto the blockchain [8].

3. RESULTS

3.1. **Encryption.** Whenever a file is added to the peer-to-peer network it will go through a cryptographic algorithm that assigns it a hash value. If a user wanted to share this file across the cloud, another user would need the hash value to access it, but this can cause a security concern since anyone can access and manipulate the file as long as they have the hash value. To prevent this, we need to implement private and public keys. When created these keys are created in pairs and thus for every public key there is a corresponding private key. The public key may be known by the public, but the

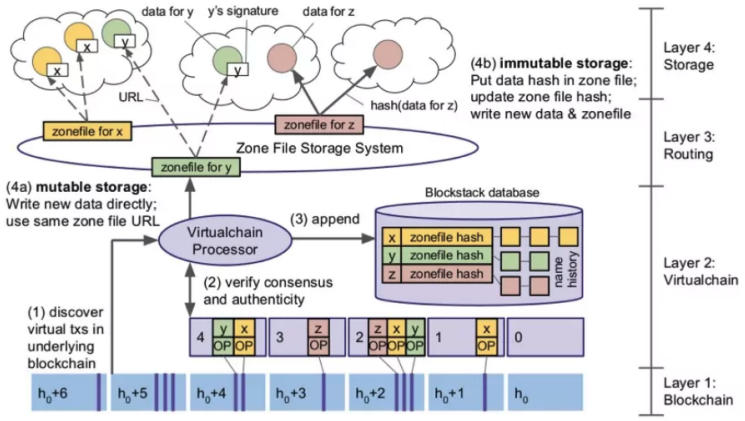

FIGURE 7. Blockchain Based File-Storage

private key is intended to be only by its respective owner. Thus, if person A now wants to share a file with person B they would use person B's public key to encrypt the file. Person B is now the only person, other than person A, who can view this file through their private key. Any malicious party would not be able to decrypt the same file because they don't have person B's private key. Rather than storing the large volumes of data associated with these files onto the blockchain, we simply store the hash values of the respective files onto the blockchain. This way we can combine the file storage on the network with a public ledger that is able to identify the cloud's records.

4. Conclusion

Blockchain is a shared public ledger that grows accordingly to its confirmed transactions that are validated by other users in the network. Originally introduced by Satoshi Nakamoto for its main use of cryptocurrency called Bitcoin [13], blockchain has shown to be a valuable solution for a secure and reliable environment. When discussing on-demand resources being delivered over the internet through cloud computing, the issue of data integrity and security arises from a centralized system. In this paper we discussed the blockchain framework and combined it alongside a cloud environment that uses a decentralized framework in order to demonstrate the key properties of blockchain that ensures data immutability, transparency, and security.

Statements and Declarations

The authors declare that they have no conflict of interest, and the manuscript has no associated data.

References

[1] Bitcoin mining. https://www.investopedia.com/tech/how-does-bitcoin-mining-work.
[2] Blockchain facts. https://www.investopedia.com/terms/b/blockchain.asp.
[3] Cloud computing explained. https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud.
[4] Cloud computing models. https://uniprint.net/en/7-types-cloud-computing-structures.
[5] Combining blockchain and file storage might just decentralize the internet. https://hackernoon.com/combining-blockchain-and-file-storage-might-just-decentralize-the-internet-d94c2701a8fa.
[6] Decentralized cloud storage solution. https://www.devteam.space/blog/how-to-build-a-decentralized-cloud-storage-solution-like-storj-io.
[7] Enterprise ethereum alliance. https://www.investopedia.com/terms/e/ethereum-enterprise-alliance-eea.asp.

[8] Learn to securely share files on the blockchain with ipfs. https://mycoralhealth.medium.com/learn-to-securely-share-files-on-the-blockchain-with-ipfs-219ee47df54c.

[9] M. Abughazalah, W. Alsaggaf, S. Saifuddin, and S. Sarhan. Centralized vs. decentralized cloud computing in healthcare. *Applied Sciences*, 14(17):Article ID 7765, 2024.

[10] J. Fadhil and S. R. Zeebaree. Blockchain for distributed systems security in cloud computing: A review of applications and challenges. *The Indonesian Journal of Computer Science*, 13(2):1576–1605, 2024.

[11] A. Javadpour, A. K. Sangaiah, W. Zhang, A. Vidyarthi, and H. Ahmadi. Decentralized ai-based task distribution on blockchain for cloud industrial internet of things. *Journal of Grid Computing*, 22(1):Article ID 33, 2024.

[12] L. Lin, J. Wu, Z. Zhou, J. Zhao, P. Li, and J. Xiong. Computing power networking meets blockchain: A reputation-enhanced trading framework for decentralized iot cloud services. *IEEE Internet of Things Journal*, 11(10):17082–17096, 2024.

[13] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[14] J. H. Park and J. H. Park. Blockchain security in cloud computing: Use cases, challenges, and solutions. *Symmetry*, 9(8):Article ID 164, 2017.

[15] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang. The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21, 2018.

[16] N. Sanghi, R. Bhatnagar, G. Kaur, and V. Jain. Blockcloud: Blockchain with cloud computing. In *2018 International Conference on Advances in Computing, Communication Control and Networking*, pages 430–434, ICACCCN'18, Greater Noida, India, 2018. IEEE.