National College of Ireland

Cloud Infrastructure Management - CIM

Futuristic 2025 Blockchain Data Centre for the Secure Network Authentication and Data Controlling and Monitoring

Nishitha Salla, x19194889
Hema Potti, x19158165
Ritesh Aswin Raam Sivagangi Gopinath, x19154160
Cloud Computing Department

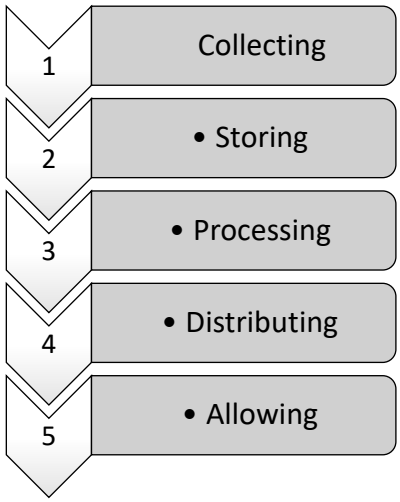
Abstract:

There are significant advancements in the technology. Every year, there are new innovative techniques developed in the field of Information Technology (IT) which helps other sectors to get benefited from the innovative technology. It is to be noted that data/information plays a vital role in any sector. There should be a lot of techniques to be developed in order to overcome the storage and security issues. The place where the data is stored, controlled, monitored, managed, and secured is called a "Data Centre". Data centre is a centralised network centre for the data management. In the data centre, networking, controlling, and monitoring plays a very important role for the data management. There have been many theoretical and practical techniques were proposed for the improved network structure in the data centre.

Considering the prominence of data centre networking, in this paper, a novel futuristic 2025 data centre with the integration of Blockchain Technology for the better networking, controlling, and monitoring of data management is introduced. This paper discusses the traditional data centre networking, controlling, and monitoring structure, introduction to blockchain technology and its impact on the data centre, a novel sample blockchain architecture, and the future recommendations of the proposed technology.

1. Introduction:

Data centre can be described as a centralised location where the networking and computing equipment is concentrated for the data management. There are 5 stages of data management which include:

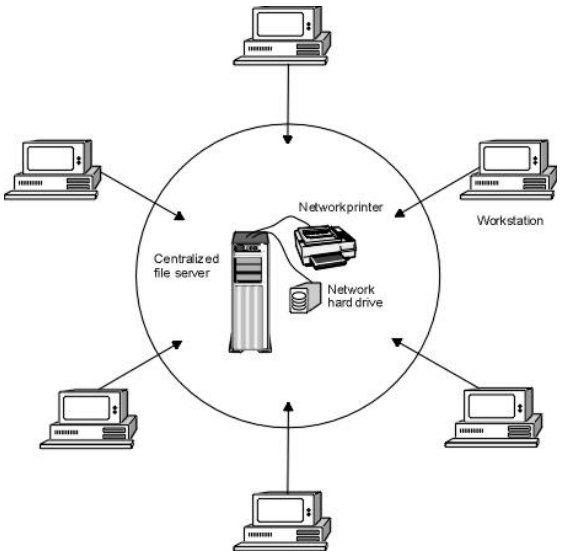


These days the data traffic is rapidly increasing which is difficult to control and monitor and thereby making the networking difficult. Though, in some cases, supercomputers are used for the data management, controlling, and monitoring the data is difficult to manage. Data centres work on a centralised network [1].

2. Centralised Network with Advantages and Disadvantages:

Centralised network is one of the types of network structure where all the users and computers will connect to a centralised

server. The central server will act as the communicating agent to all the computers and users. Centralised network is the most common type of network used these days for the collection, storage, and processing of data. Centralised architectures are build and deployed for the management of entire network.



However, there are many advantages and disadvantages of using centralised network.

The advantages include:

1. An authorised chain of command: All the employees of the organisation will have a clear idea of whom to reach out in case of any disaster. A clear plan can be executed by the senior authorities of the organisation based on the centralised network structure and thereby making the decisions quickly and precisely [2].
2. Focused Vision: Using the centralised network, organisations will have a clear vision of their work structure.
3. Physical security of the network and computing equipment is more precise.
4. All the organisations and users will have dedicated servers and resources such as memory, CPU etc. [2].
5. All the services can be managed in a centralised location for any quick updated and patches.

However, the centralised data centres have got a lot of *disadvantages which include [3]:*

1. Since the entire process is centralised there will be a lot of working pressure from the data centre end which would make control over the data much difficult.
2. All the computers and users are connected to the central network which will increase the network traffic there by increasing the load on the network.
3. In case of any failure such as network issues, any natural disasters, downtime, etc., the entire network/service will be down. This type of scenario is called SPF (Single Point of Failure) which is the most common type of failure in the centralised networks.
4. Centralised networks are more versatile for being hacked as there are many attacks noted till date such as DoS and DDoS. The attacks are quickly described as over flooding the network with malicious or unnecessary data in order to compromise the target systems.
5. With increase in data, number of servers will also increase there by increasing the maintenance work, operational and indirect costs.
6. It would be very difficult for the network and system administrators to control and monitor the huge amounts of data being redirected to the centralised location and there by getting difficult to detect the attacks.
7. In the centralised networks, the data can be replicated in a couple of regions. In case of technical glitches or

attacks, the data will be lost, thereby reducing the high availability.

8. Security is one of the major issues in the centralised networks as the data is centralised at one point using same operating systems which are more versatile for being hacked.

Thus, the centralised network has more disadvantages. In order to overcome the current network, controlling and monitoring issues, Blockchain Technology is introduced in this paper.

3. Blockchain Technology:

Blockchain is a decentralized network with distributed ledgers. It is first developed for the purpose of crypto currency. But, in the later stages, the blockchain technology has got a lot of prominence and is used in many sectors which include IT, law, supply chain, finance, banking industry etc. Though the blockchain technology is developed based on the decentralized network, a lot of robust algorithms are developed for validating and encrypting the data. Before discussing the robust algorithms, it is important to discuss the pillars and elements on which the blockchain is developed.

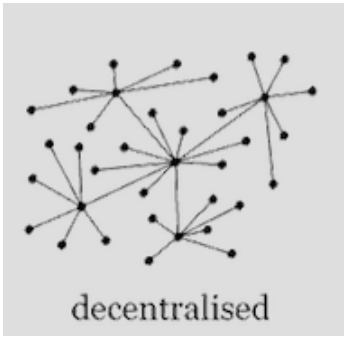
3.1. Pillars of Blockchain Technology:

The blockchain is developed on three main pillars which include [4]:

a. Decentralisation
b. Immutability
c. Transparency

a. Decentralisation:

Decentralised network is developed for the no SPF (single point of failure) and is a trustless environment. The data in this network is distributed among the users and computers. All the users in the network will have access to the data being transmitted on the network. In centralised network, the authority and responsibility of the data will be with the network and system administrator on the data centre end, however, in the decentralised network, all the users on the network share the equal responsibility and authority over the data. All the computers on the network will act as a server by itself there by increasing the fault tolerance and high availability as the data is stored in every computer, where as in the centralised network, the data is stored at a central point for which the fault tolerance and availability might not be high in case of any issues or attacks. During disasters, technical issues, or cyber-attacks, data stored in the centralised network will be lost and will be a difficult task to retrieve if there is no back up [4].



b. Transparency:

The second pillar of the blockchain is transparency which is defined as “data being transparent to all the users in the network while transmitting or at the state of rest”. In the blockchain technology, transparency is particularly restricted to view the sender user credentials. However, all the users in the network can view receiver identity, time stamp, data being sent and the sender identity (all in an encrypted format). Below is the sample example of transparency:

Say, in the traditional data centres, if the sender sends the data, the data encryption depends on what type of protocol is used on the network and tracking the data will be one of the most difficult parts as it is unsure where the data will be stored on the data centre end. A group of users on the network will not have direct access to the data stored on the database there by making it difficult for them to identify and detect any fake information and attacks. However, in the blockchain technology, the information is transparent making the technology robust tracking and monitoring the data [4].

c. Immutability:

Immutability is one of the most important and robust pillars on which the blockchain technology is built. It can be defined as "The data being transmitted on the network is formed as a block (blocks will be formed based on the data being transmitted on the network) which cannot be tampered or changed at any instant of time". This provides an additional security for all the blocks created o the network. In the traditional centralised network, data tampering is one of the major issues as the hackers can tamper the data and can steal, spoof, and destroy them for any purposes, when this happens, no user on the network will be notified during the attack making this more vulnerable. However, in the blockchain technology, it is impossible to tamper the data as all the users in the network will be notified immediately based on the hash values present on each block [4].

3.2. Elements of Blockchain Technology

There are five major elements on which the blockchain technology is built. They are [5]:

a. Encryption
b. Immutability
c. Tokenisation
d. Decentralisation
e. Distribution

a. Encryption:

Encryption plays a major role in the blockchain technology. The encryption is carried out by the private and public keys. They are used for encrypting the data into 256 hexadecimal format i.e. a 32 bytes or 64 character in range. The encrypted information will be shared among the users on the network. However, no personal information of any user will not be shared [5].

b. Immutability:

Immutability is a pillar and an element in building the blockchain technology. (Immutability is explained in the previous section) [5].

c. Tokenisation:

The information exchanged between the users on the network will be shared in the form of Tokens. Tokens will contain the metadata which might be any updates, upgrades, transactions etc. being carried out on the network. All the users will have tokens based on the data transmission on the network which makes the network robust [5].

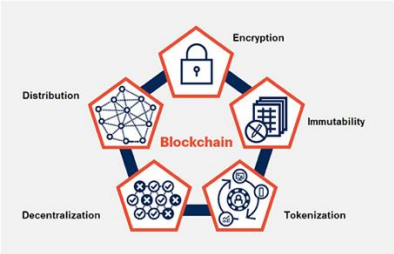
d. Decentralisation:

Decentralisation is also one of the elements on which the blockchain technology is built apart from being one of the pillars. Decentralisation is explained in

the previous section 3.1. [5]

e. Distribution

All the users on a network need to be at the same location. They can be at different locations, connect to the same network, distribute the created ledgers, and maintain an individual copy of ledgers and blockchain information.

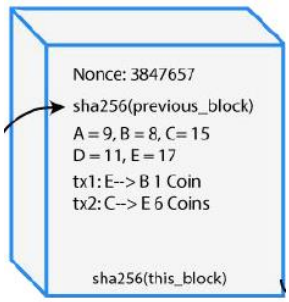


Thus, blockchain is developed on robust pillars and elements.

3.3. Blockchain Components:

As discussed in the previous sections, once the data is transmitted on the network, the data will be formed as a block. In this section, the components present in the block will be discussed. Blocks created in the blockchain formation process are [6]:

a. Metadata
b. Hash of the current block
c. Hash of the previous block
d. Nonce
e. Time-stamp
f. Block size
g. Type of encryption algorithm



a. Metadata:

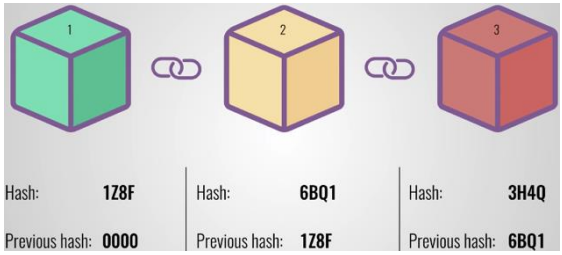
In general, the metadata consists of the data being sent and received on the network.

b. Hash of the current block:

Hash is a unique number created when the data is encrypted which has a fixed length. When the block is created, the hash value will be present in the block [5].

c. Hash of the previous block:

In the blockchain technology, the hash of the previous block will be shared with the current block, and the hash of the current block will be shared with the next block, thereby making the whole blockchain created robust and impossible to hack or attack [5].



d. Nonce:

A nonce is a unique number created by the user when the block is created. The nonce will further be validated by the other users on the network in order to make sure that the block is original [5].

e. Time-stamp:

Time-stamp is the time when the block is created and uploaded to the blockchain.

f. Block size:

When the block is created, it is important to know the size of the block, which will also be added as the block component.

g. Type of encryption algorithm:

The encryption algorithm used in the blockchain technology is SHA256 (Secure Hash Algorithm 256 where the 256 represents the number of bits). This will be formed in a hexadecimal format. SHA 256 encrypts the data and is added to the block which is immutable [5].

3.4. Validating Algorithms

There are three validating algorithms in the blockchain technology which include:

a. Proof-of-Work
b. Proof-of-Stake
c. Delegated Proof-of-Stake

a. Proof-of-Work:

In terms of IT, proof-of-work can be defined as uploading the data to the block and being validated in general. The data could be in general and is validated by the security applications and the services on the computer.

b. Proof-of-Stake:

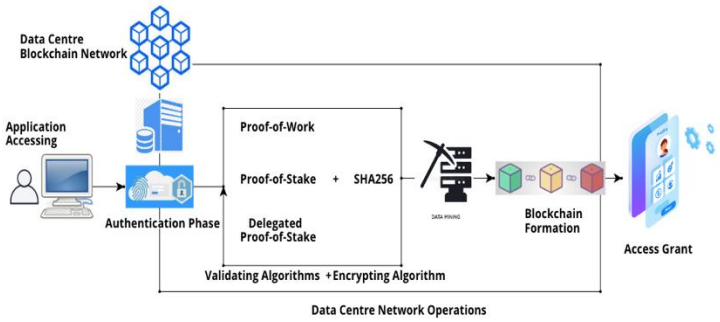
This validating algorithm in general is used for the cryptocurrency by validating the transactions and distributing the rewards based on the number of stakes the minors in the network own. In IT, this validating algorithm is not particularly used.

c. Delegated Proof-of-Stake:

This validating algorithm is used based on the validating the data from both the customer and data centre end. This is most commonly used algorithm for validation.

4. Novel Blockchain Data Centre Architecture

Blockchain is considered as the novel platform for developing the data networking, controlling, and monitoring structure. A novel blockchain architecture is developed for the secure authentication purpose for the developed network, controlling and monitoring structure from the data centre end. The novel architecture developed is represented as:



The developed architecture is planned to improve the robustness of the network structure and provide better controlling and monitoring options for the users on the network. The process can be described as:

Step 1: When the user/customer tries to login to an application, they must provide their credentials i.e. their username and the password. Once they provide their details, the credentials will then be redirected to the data centre (in an encrypted format) where the application server is mounted.

Step 2: Once the credentials are redirected to the server end (i.e. data centre), the credentials will be then validated using the validating algorithms. The proof-of-work algorithm will validate the data entered and delegated proof-of-stake algorithm will be used by the group of users on the network for validating the data transmission alongside the validation of data.

Step 3: Once the data is validated, the data will now be encrypted using the SHA256 encryption algorithm which is an extra layer of security encryption which in turn makes the network more robust.

Step 4: Once the data is validated and encrypted, in this step, the data mining takes place. Data mining is described as adding the whole process of authentication process in the form of block which will be transparent and immutable in nature as per the blockchain

development. The data will be distributed to all the users on the network in an encrypted format which will make easy for the users to monitor the data in order to prevent the attacks there by controlling the data.

Step 5: In this step, after the data mining, the data will now be formed as a block which contains the block components mentioned in the section 3.3.

Step 6: In this step, the credentials of the user/customer trying to access the application will be grant access.

The process of validating, encrypting, mining, and blockchain formation will be from the data centre end making the networking, controlling, and monitoring robust.

Conclusion:

There must be a lot of techniques developed for improving the networking structure and for controlling and monitoring the data being processed at the data centres. With increase in attacks on the centralised networks, there is a lot of necessity to introduce new techniques.

In this paper, blockchain technology is chosen for developing a robust platform for the data centre networking and for controlling and monitoring the data. A novel architecture is also developed for which includes the process of authentication and provides the insights of improved network, controlling and monitoring.

Limitations and Future Works:

The most important part of developing the a blockchain platform is based on the use case. The use case for the futuristic 2025 data centre is a perfect match for the proposed technique. However, the technique is limited to the networking, controlling and monitoring structure of the date centre, and for the authentication purposes. In future, based on the blockchain technology, it can be planned to integrate AI and other robust platforms to the technology for the better results.

References:

1. Bernadette Johnson. 2019. What is a data center? [Online]. [15 April 2020]. Available from: https://computer.howstuffworks.com/data-centers1.htm

2. Cfi. 2019. Centralisation. [Online]. [14 April 2020]. Available from: https://corporatefinanceinstitute.com/resources/knowledge/strategy/centralization/

3. Matt mcgew. 2018. The Disadvantages of a Centralized Network Scheme. [Online]. [14 April 2020]. Available from: https://itstillworks.com/disadvantages-centralized-network-scheme-12213044.html

4. Parikshit hooda. 2018. Comparison – Centralized, Decentralized and Distributed Systems. [Online]. [14 April 2020]. Available from: https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/

5. Ameer rosic. 2017. Blockchain Technology. [Online]. [15 April 2020]. Available from: https://blockgeeks.com/guides/what-is-blockchain-technology/

6. Kasey panetta. 2019. The CIO's Guide to Blockchain. [Online]. [15 April 2020]. Available from: https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/

***