Design and Implementation of a Blockchain-Enabled Cloud Architecture for Accelerated User Transactions

[1]V Uday Kumar, [2]Kaila Shahu Chatrapati
[1]*Research Scholar, JNTU Hyderabad, India.*
Email:uday009u@gmail.com
[2]*Professor , Department of CSE, JNTU, Hyderabad, India*
Email:shahujntu@gmail.com

KEYWORDS

Blockchain, Global Ledger, Validators, Miners, Hash tree, Merkley tree, SHA256

ABSTRACT

Over the years, Centralized Systems are servicing billions of people all around the world. Most of the today's popular applications like Facebook, Twitter, Instagram, Amazon, Google etc. are based on centralized systems. There are few disadvantages of centralized systems. The first disadvantage is that if the central system fails, the entire system may become inaccessible, leading to complete downtime. The second disadvantage is as the system grows, the central node can become a bottleneck, struggling to handle increased loads efficiently. This can lead to delays and degraded performance. The third one is about security. If someone hacks central system, the entire customers data may be compromised. Unlike centralized systems, Blockchain allows to distribute data among all nodes preventing single point failure. Since the data is distributed and each blocks have their own hash key linked with other, its merely impossible to tamper a transaction. Blockchain can be easily scalable when compared to centralized systems. In this paper, we design and implement BAF (Blockchain Architecture for Fast execution of transactions). We select only fewer number of users ledger to update the transactions. Multithreading is used to perform write operation on selected ledgers. The experimental results showed that proposed work reduced 28% of execution time of user transactions at an average case.

.

1. Introduction

Today's applications are centralized applications. Data is stored in a central location which is also called a powerful computer device, a server. Some of the popular applications are Facebook, Google, WhatsApp, Twitter, Amazon, Netflix etc. There are few drawbacks of centralized systems. First is single point failure, second is Scalability, third is security.

Single point failure: - In a centralized system, data is stored in a powerful computer device called as server. This may fail because of many factors like network failure, hardware failure, natural disaster like earthquake etc. If data is not replicated in another server which is located in different location, then the loss is major and almost impossible to recover the data lost.

Scalability: - As the application grows, it is very important to maintain the same level or improved level of efficiency. That is, it is important to scale the application. Unfortunately, in centralized systems, it's not an easy job to achieve.

Security: - Though the applications are protected using anti-virus software's and firewalls, still hackers come with novel approaches to hack the server. As the entire data is stored in one single device, if they target that device which is also called as server then the entire data may be compromised.

Billions of people trust these centralized systems in spite of above said three drawbacks. Alternatively, we have Blockchain technology which is decentralized system. This may not immediately replace all of the above-mentioned popular applications which are in use till today but may rule out after a decade or so. The below is an example to distinguish how centralized system and decentralized system works.

Let's consider the following table which is stored in centralized database

Users	Wallet Balance
A	15
B	25
C	12

Table 1 : user's data

Now consider if user A wants to send 5 units to C. The user A initiates the transaction as

Tran ID	sender	senders balance	receiver	Units to transfer	Timestamp
1001	A	15	c	5	24/10/2024 16:48:52

Table 2 : Transaction details

After executing above transaction, the database is updated in central location as

Users	Wallet Balance
A	10
B	25
C	17

Table 3 : User's accounts

Banking systems till today follows as shown above. People trust banking systems. For an instance let's consider that central server is compromised to user A. User A can easily the wallet balance by modifying all transactions with wrong values. Such scenarios in real work may be rare but may happen any time. This happens because users accounts are maintained globally in a single device. Let's call it as global ledger where all transactions are recorded. In Blockchain technology, every user will have their own ledger where all transactions are recorded as shown below.

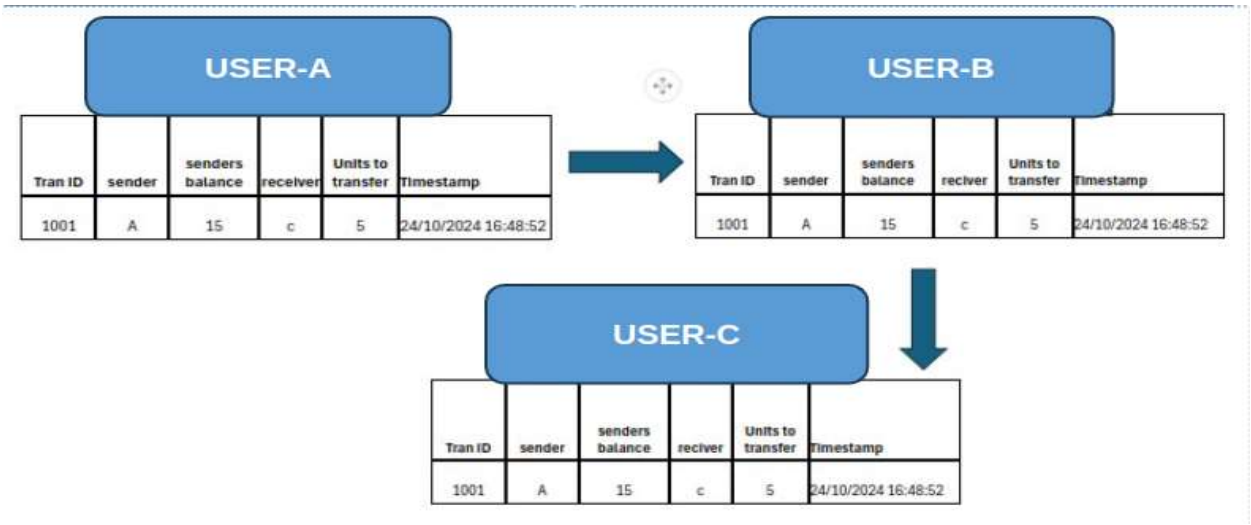

Figure 1: Decentralized system

All the users have an individual record of transaction made. Even if user A's node is compromised, it's impossible to change the entries in all user's ledgers. The protection is ensured using hash value. If we make any transaction then hash value of that block is changed and to maintain the chain consistently, remaining ledgers hash values have to be changed. Achieving this is not possible because for every transaction there is a time limit to execute. For example, Bit coin which uses Blockchain technology maintains a time limit of 10 minutes for transaction execution. If anyone wants to tamper a transaction, it's impossible to update all ledgers in the Blockchain in just 10mins, instead this job may take hours of time. This is biggest advantage of blockchain when compared to decentralized systems. Another advantage is it is easily scalable. That is adding new nodes and blocks are easy. Hence, not only Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner [1] but also easily scalable.

In order to generate hash value for each transaction, SHA256 algorithm is used and a hash tree or Merkley tree is used to create block level hash value. A Block level hash is created whenever a single transaction entry is made in a block.

2. Background Study

Blockchain Technology came into existence during 2008. Blockchain technology is a decentralized and distributed digital ledger that records transactions across multiple computers in a secure and tamper-proof manner. Each transaction is stored in a block, and these blocks are linked together in chronological order to form a chain, hence the term blockchain. The key elements in Blockchain architecture are Nodes, Users, ledger, blocks, transactions and hash values. Each node may have one or more users. Each user will have a ledger called as Blockchain. It has Blocks with fixed size. The transactions data is written on blocks. They are connected with hash values.

In 2019, a paper published by Wenli Yang & Co. aimed to address blockchain integration to secure Internet services and identify the critical requirements of developing a decentralized trustworthy Internet service [3]. In 2018, a paper published by Shitang Yu & Co addressed High performance Blockchain platform that achieves efficient connection of intelligent devices through the node-to-node mapping mechanism [6]. In 2021, a paper published by Muhammad Nasir Mumtaz Bhutta

& Co performed a comparative analysis of frameworks, classification of consensus algorithms and analysis of security risks & cryptographic primitives that have been used in the Blockchain so far [4]. In 2023, a paper published by Saminur Islam & Co. investigated operational and interoperability issues in existing blockchain-based applications to understand challenges and provide recommendations for future developers [5]. In 2024, a paper published by author Yao-Chung Chang & Co proposed a security mechanism using private blockchain system [7]. In 2024, A text book written by authors Asraf S and Shiva Das titled Blockchain Technology Algorithms and Applications [8] provided comprehensive details about Blockchain algorithms and its applications.

2.1 Key Features:

Decentralization: Data is not stored on a single server but is distributed across a network of computers (nodes).
Immutability: Once a transaction is recorded, it cannot be altered or deleted, ensuring transparency and security.
Transparency: All participants in the network can view the transactions, making it a trustless system.
Security: Transactions are encrypted and validated using cryptographic methods.
Consensus Mechanism: Transactions are verified by all nodes in the network using mechanisms like Proof of Work (PoW) or Proof of Stake (PoS).

Designing blockchain-based applications is a challenging task and requires a number of coordinated architecture decisions . Few major Blockchain platforms are as follows.

- Bitcoin: Primarily for cryptocurrency transactions.
- Ethereum: Supports smart contracts and decentralized applications (DApps).
- Solana: Known for high transaction speed and low fees.
- Polkadot: Facilitates interoperability between different blockchains.
- Cardano: Focuses on scalability, sustainability, and security.
- Tezos: Self-amending platform for DApps and smart contracts.
-

3. Proposed work

In this work, BAF (Blockchain Architecture for Fast execution of transactions) is implemented. The objective is to perform write operation on only selected users ledger but not in every ledger of the user and also the write operation on selected users ledger is done parallelly using multi-threading. By doing so, the same security levels are preserved. Selection of users is done by using randomized algorithm. The transactions are written only on those users' ledgers at a time using multiple threads. This can definitely save execution time of transaction.

3.1 Proposed Architecture

The following Figure 2 shows the proposed architecture. The component RMW is Randomized algorithm with multi-threaded enabled write operation on blocks. As an instance, validators are shown as C, G.

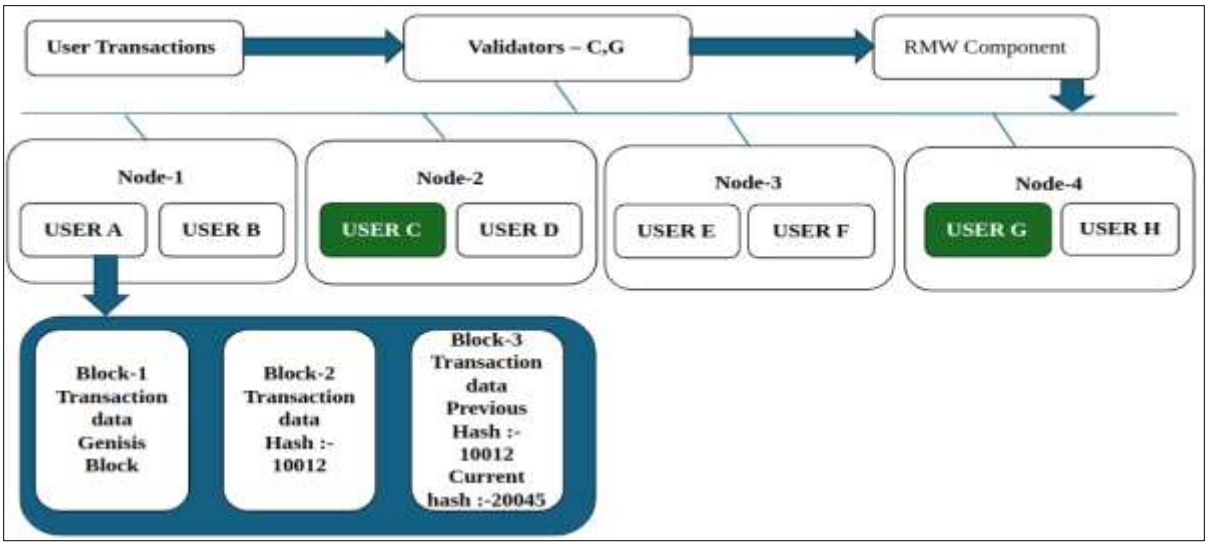

Figure 2 Proposed BAF architecture

3.2 Steps to execute transaction in proposed work

1. User logs in using Private key.
2. Initiates transaction with parameters transaction-id, sender, senders balance, receiver and number of units to transfer, timestamp
3. Transaction is broadcasted to all validators or minors to validate a transaction. Who are honest participants and stake holders who earned good number of shares to become a validator or miner.
4. Validators validate the transaction by verifying whether sender and receivers are part of network and authorized to perform a transaction or not. If sender is authorized to perform transaction, then validators checks whether sender has enough funds to transfer the amount.
5. Once the transaction is validated then it is broadcasted to selected users using randomized algorithm. The transaction is written in last block of their blockchains using multiple threads. Note that by default, sender and receiver ledgers are also selected including users selected by randomized algorithm.
6. Transaction details are written in last block of all users (sender, receiver and randomly selected users other than sender and receiver). Every block has some fixed size. In this work, block size is 512kb. If size of last block is full then a new block is created. SHA256 is used to generate hash values. The hash values are generated to all the transactions of a block in which new entry is made. Later hash tree is constructed to generate a block level hash value.
7. Senders and Receivers wallet balance is updated and transaction is successfully completed.

After completion of transaction, it's impossible to know which users were selected randomly by the algorithm. Which means transaction once done cannot be modified by anyone without reading each and every users data in blocks. This will disable the activity of the user immediately as this operation cannot be completed in a specified time limit.

3.3 Algorithm : Execute Transaction

Void execute_transaction(sender, receiver, amount, timestamp, balance)

Start :

Declare :

Boolean Validated;
Integer X ; // number of users in the network
Integer K to store number of users to be selected by randomized algorithm.
// K is a threshold which depends on number of users X. Eg if number of users are 100, K could be some defined threshold 10. Let N be an array of objects to store user-ids selected by randomized algorithm, Node number of selected user.
Integer M be the number of validators or miners in the network.
Begin :
C=0;
for (int i=1 to M) : // each miner
if(senders_balance > amount to be transferred)
c++;
End for;
If(c==M)
Validated= true;
Else
Validated=false;
Terminate the transaction ;
for(i=1 to K) :
j= randamozed(min_id, max_id)
if (j==senderid or receiversid)
repeat above loop to generate different id.
else
Initialize N[i].userid, N[i].Node-number;
End for;
For(i=1 to K)
Thread Ti = new Thread;
End for;
// K number of threads are created such that T1 works for user1 ledger.
For each thread – void run ()– thread function :
If last block of ith user is full then create a new block
Write(transaction details)
End thread run method;
Write(transaction details) in senders and receivers ledgers
for (i=1 to K) :
for all transactions of user i in last block, create hash values
Generate_hash-SHA256(transaction-details-of-user-i);
Generate_block_hash(transaction-hashvalues);
End for;
Update sender and receiver's wallet balances
// Transaction complete;
End;

The above function execute_transaction() takes O(K) time where K is the number of selected users using randomized algorithm. To produce a random number which is considered as user identification number takes only constant time. To read transaction details of all users then entire block chain has to be read from all the nodes in the network. Based on authorization, users can perform read operation on their own node to check their transactions. Time to perform read operation depends on size of blockchain in a node.

The following example illustrates how block level hash values are updated using hash tree.

A hash tree also called as Merkley tree data structure is used to generate block level hash value. Its bottom-up tree.

Let A,B,C,D are four transactions. Individually for each transaction, hash values are generated using SHA256 algorithm. Those hash values are child's, intermediate nodes are generated by concatenating the parent level hash values. Finally root node hash is generated by intermediate nodes hash values and hash value of previous block.

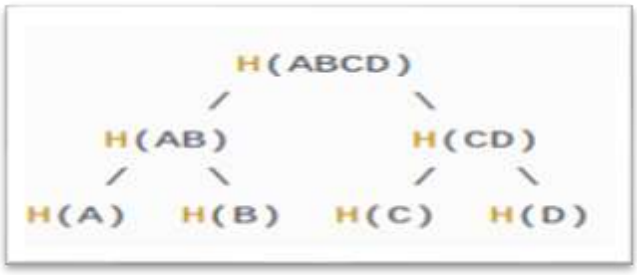

Figure 3: Hash tree to generate block level hash value

Evey block the following block header information

1. Block hash value in 256 bit binary number represented in Hexa decimal number
2. Hash value of previous block – represented in Hexa decimal number
3. Block time stamp – the time at which block is created

4. Experimental results

The architecture is implemented using virtual machines. 5 virtual machines are created. Each machine is referred as a node. Each node as 5 users. That is a total of 25 users with their own blockchains are participating in the network.

A total of 500 transactions of users from different nodes were selected to conduct experiments. First four transaction details are shown in below Table.

Tran ID	sender	senders balance	receiver	Units to transfer	Timestamp	Node-id
12145	A	78	E	15	18/10/2024 16:48:52	1
12487	D	48	B	10	11/10/2024 8:48	3
11567	B	64	G	20	8/5/2024 14:04	2
12589	G	125	A	15	25/10/2024 16:48:52	1

Table 4 :- Transaction details

The following table illustrates the execution times recorded for each transaction in minutes using Traditional Blockchain architecture and proposed work BAF.

Traditional Blockchain		Proposed BAF	
Transaction-Id	**Time in minutes**	**Transaction-Id**	**Time in minutes**
12145	2.15	12145	1.41
12487	2.18	12487	1.56
11567	2.37	11567	1.38
12589	2.21	12589	1.47
13548	2.04	13548	1.18

Table 5:- Experimental Results of first five transactions

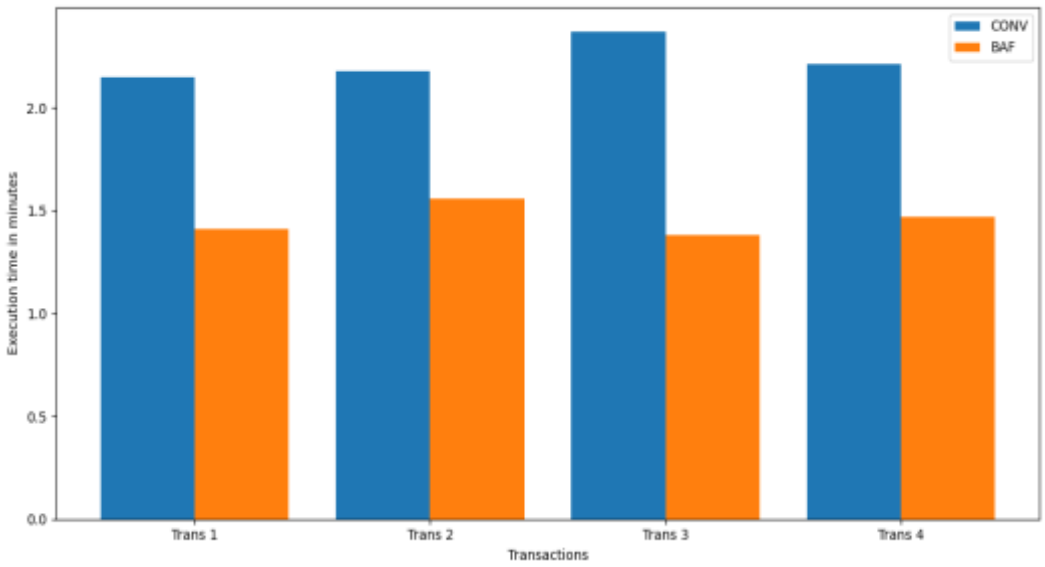

Figure 4 : Comparision of Conventional approach with Proposed BAF

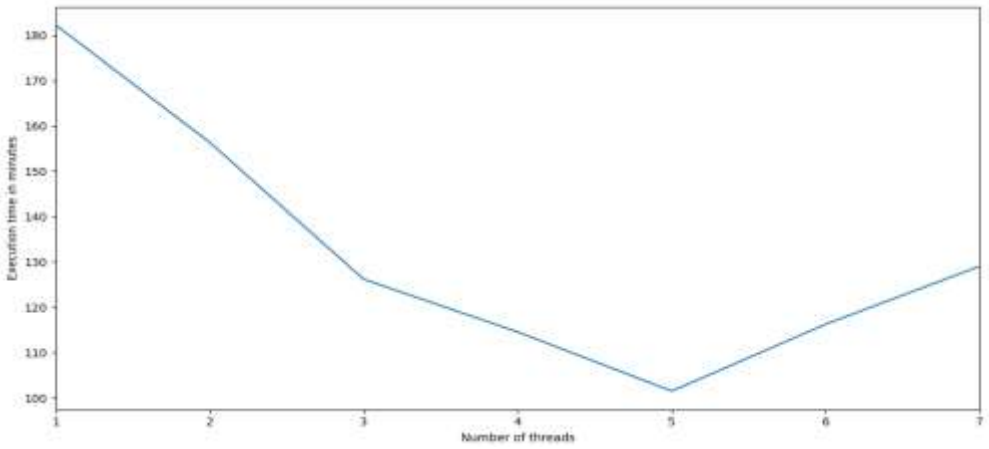

Figure 5: Performance of Multi-threading X-axis number of threads and Y-axis Execution time in minutes

Conclusion

In traditional Blockchain architecture, every user will have their own blockchain. Users' transaction execution takes place in all blockchains of users participating in peer-to-peer network. In this paper, we designed and implemented a novel approach to execute user transactions quickly. We used a randomized algorithm to pick few users randomly for every transaction, allowing us to perform write operation on only selected user's blockchain. By doing so, the same security is maintained like traditional blockchain technology. That is, if any one tries to tamper a transaction which was already happened, then entire blockchain hash values have to be updated. We used hash tree similar to Merkley tree to construct block level hash. We experimented with 20 user transactions. The experimental results showed that user transaction execution time is reduced at an average by 28%. Further more research is required to generate block level hash value more efficiently because the block level hash value changes for every change that made in a block.

References

[1]. Zibin Zheng, Shaoan Xie , Hongning Dai , Xiangping Chen , and Huaimin Wang3 , "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE, 2017.

[2]. Maximilian Wöhrer , Uwe Zdun , "Architectural Design Decisions for Blockchain-Based Applications" , IEEE, 2021.

[3]. Wenli Yang , Erfan Aghasian , (Member, Ieee), Saurabh Garg , (Member, Ieee), David Herbert, Leandro Disiuta, (Member, Ieee), And Byeong Kang, "A Survey On Blockchain-based Internet Service Architecture: Requirements, Challenges, Trends, And Future" , IEEE, 2019.

[4]. Muhammad Nasir Mumtaz Bhutta 1 , Amir A. Khwaja1 , adnan nadeem 2 , (member, ieee), hafiz farooq ahmad3 , muhammad khurram khan 4 , (senior member, ieee), moataz a. hanif5 , houbing song 5 , majed alshamari1 , and yue cao , " A Survey on Blockchain Technology: Evolution, Architecture and Security " , IEEE, 2021.

[5]. Saminur Islam 1 , Mohammad Jaminur Islam shahid noor4 , kyung-sup kwak 5 , (life senior member, ieee), And S. M. Riazul Islam , " A Survey On Consensus Algorithms In blockchain-based applications: architecture, taxonomy, and operational issues" , IEEE, 2023.

[6]. Shitang Yu, Kun Lu, Yingcheng Juo, Jun Zuo, Bo Zhang, "A High Performance Blockchain Platform for Intelligent Devices" , IEEE, 2018.

[7]. Yao-Chung Chang a, Yu-Shan Lin b, Arun Kumar Sangaiahc and Hsin-Te Wu , " A Private Blockchain System based on Zero Trust Architecture", IEEE, 2024.

[8]. Asraf S, Shiva das Neelima, 'Blockchain Technology Algorithms and Applications', Wely publications, First edition, 2023.