DOI: 10.15849/IJASCA.230320.07

Int. J. Advance Soft Compu. Appl, Vol. 15, No. 1, March 2023
Print ISSN: 2710-1274, Online ISSN: 2074-8523

Using Consensus Algorithm for Blockchain Application of Roaming Services for Mobile Network

Ahmad al-Qerem[1], Ala Hammarsheh [2], Ali Mohd Ali1[3], Yasmeen Alslman[4] , Mohammad Alauthman[5]

[1]Department of Computer Science, Faculty of information technology, Zarqa University, Jordan
ahmad_qerm@zu.edu.jo
[2]Computer Systems Engineering, Faculty of Engineering, Arab American University, Jenin, Palestine
ala.hamarsheh@aaup.edu
[3] Communications and Computer Engineering Department, Faculty of Engineering, Al-Ahliyya Amman University, Amman, Jordan.
a.mahmoud@ammanu.edu.jo
[4] Department of Computer Science, King Hussien School of Computing, PSUT University, Jordan
yas20188012@std.psut.edu.jo
[5]Department of Information Security, University of Petra, Amman, Jordan
mohammad.alauthman@uop.edu.jo

Abstract

Blockchain technology has recently emerged as one of the most innovative solutions on the market. It is predicted to become as popular as the internet was in its early days during the 1980s. With the use of a consensus algorithm, the blockchain creates a cryptographic record that is unalterable. The system uses a combination of repeated sequence hashing and failure tolerance to achieve this outcome. Decentralization, immutability, anonymity, and accountability are just a few of the key features of blockchain. Due to these attributes, many businesses in various industries are now exploring the possibility of incorporating blockchain into their IT systems. Consensus algorithms are a vital component of blockchain technology and play a crucial role in ensuring the reliability and efficiency of the blockchain. The Raft Consensus prevents the generation of new blocks until transactions are confirmed. This also saves storage space, particularly during periods of low transaction activity, as unoccupied blocks do not consume storage space. To evaluate the efficiency of the Raft consensus algorithm, a simulation of a roaming services application for mobile network operators (MNOs) was performed. This simulation assessed the blockchain's efficiency in terms of network performance. The results indicate that implementing this technique could significantly increase transaction volumes.

Keywords: *Blockchain Technology, Decentralization, Raft consensus algorithm, Permanence, Anonymity, Business Integration, Mobile Network, Transaction Volume..*

Received 25 December 2022; Accepted 13 February 2023

1. Introduction

A blockchain could be considered a decentralized database of records or a public ledger of all digital transactions or events that have happened and are shared among the parties involved. Every transaction in the public ledger must be verified. Also, it cannot be removed once the information has been entered. Today's digital economy needs a trusted third party, but these parties can be hacked or manipulated in other ways. This is why blockchain technology has grown and changed.

As was already said, distributed consensus and anonymity are two of the most important and unique things about Blockchain. There are two kinds of blockchains: a public blockchain and a private blockchain. Anyone can join a public blockchain, but only the people who are part of a private blockchain know who each other is. Users can make private transactions and agreements when using a private blockchain. This study shows that the Raft consensus mechanism could be used to build a private blockchain.

Because the consensus algorithm is so important to keep the Blockchain safe and to work well, using the wrong one could hurt the performance of the Blockchain and the applications it can power. All nodes in a distributed system must be consistent, and the consensus technique ensures that they work together as a coherent group, which is important for high-quality, large-scale systems.

One of the consensus algorithms, Raft, is in charge of managing the copies of logs. The fact that it was easy to explain was a big part of how it was made. It works about the same as Paxos and can handle problems the same way. Raft is different because it breaks the problem into smaller parts and solves each one simultaneously. Once called a private blockchain, this type of network is needed to make Raft work on the Blockchain so that users can connect more easily.

Blockchain technology, which Satoshi Nakamoto first suggested in 2008 in relation to Bitcoin, has gotten a lot of attention in recent years [1]. A blockchain is a distributed database and transaction system where all peers share information. It is safe because it is not centralized.

Blockchain technology could be used for a wide range of asset transfers and point-to-point (P2P) transactions because it is decentralized and can be checked. There are now apps that use the Blockchain. These applications include commercial services [2–4], the internet of things (IoT) [5–6], supply chain management systems [7–9], and so on. Blockchains can only work in the long term if they have consensus algorithms. This is because a blockchain can be built on top of a system that doesn't have a single point of control.

In distributed systems, a consensus algorithm is used to figure out how to coordinate the work of several nodes or get the nodes to agree again if there are more than two. This is done by making a plan and then following through on it. PoW [1] and PoS [7] are just two of many Consensus algorithms being worked on now. [8, DPoS (Delegate Proof-of-Stake)] Byzantine Fault Tolerant (PBFT), Paxos, and Raft are all possible. Some examples are the prisoner and proof of stake (PoS) algorithms, which provide a strong foundation for reliability, fault tolerance, and quantification. Because of this, public blockchains can choose between proof-of-prisoner and proof-of-stake. During this time, anyone can join

the network, and there are no trust links between the nodes. Because of this, prisoner and point-of-sale systems can only be used for tasks requiring fast confirmation.

To ensure the network works "right," all participants in an overarching consortium or private blockchain network must be on a "whitelist" and agree to follow strict rules. Because of this, two other economic consensus algorithms, PBFT and Raft, are better choices. Private blockchains or consortiums can be used for many business purposes.

Hyperledger is one of the groups making blockchain frameworks for business networks [13]. Syndicates can also build their blockchains with Ethereum's tools [14]. The Raft algorithm is used in a wide range of unusual networks as a way for personal blockchains to reach a consensus. [15]

Hybrid consensus techniques are also being worked on to improve the power of consensus while keeping its ability to be measured. For example, Zilliqa [16] wanted prisoners to choose the members of the D.S. committee, which would then use the PBFT Consensus protocol on the locking block. In contrast to PBFT and Paxos, the Raft method is very fast and easy to use. Because of this, it has been used in many distributed system architectures. Ledger entries can only move from the leader to other servers in a Raft-based system. In Raft, a leader-based system, choosing a leader is a key part of the Consensus protocol.

Paxos and its better algorithms do not think of a leader as essential to the Consensus protocol. Because each node can send commands, the network can better divide the work among its nodes [11, 17]. The design of Paxos, on the other hand, needs more major changes.

Raft, a consensus algorithm that provides the same level of safety as Paxos, is designed to be simpler and more accessible than Paxos. Unlike Paxos, Raft cannot tolerate malicious nodes, but it can recover from a crash fault of the fifty-first node. These nodes refer to the computers that participate in a private blockchain. A graph for personal blockchain applications demonstrates the importance of crash fault tolerance over Byzantine fault tolerance. When more than half of the network's nodes are no longer controlled by the current leader, a network split is said to have occurred. This can result from individual node failures or packet loss, making communication within the network difficult. In such a scenario, the Raft Consensus blockchain network must restart by electing a new leader. During this time, the network will not be able to communicate with the Blockchain because the latter will not accept any new transactions.

The paper will then proceed to examine the use of rafts in the Blockchain in section V, present a system fraud prevention case study in section VI, and conclude in section VII. In section II, the concept of a working quorum will be explored in greater detail. Section III provides a comprehensive overview of blockchains and how they operate. Finally, section IV offers an in-depth examination of the Raft consensus method.

2. Background

Enterprises and researchers are exploring using private blockchains with permissioned access to help them achieve their professional objectives. Corda and Quorum are two widely adopted private blockchain platforms, with Quorum employing a vote-based consensus process. Corda, like Quorum, is a private blockchain platform. Quorum [6],

specifically designed by J.P. Morgan, aimed to leverage existing technology as much as possible in its design. This led to the implementation of Quorum around the official Go implementation of the Ethereum protocol. The project was also designed with decentralization as a goal, utilizing as much existing technology as feasible.

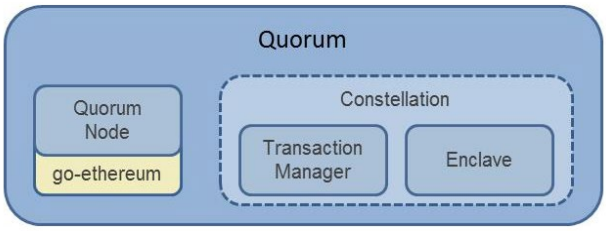

Figure 1. Quorum architecture.

Modifications to the go-Ethereum source include the blocking proposal and a way for confirming blocks. The Quorum's structure can be seen in the graphic above. Using Quorum in a business context can be done publicly or privately. [7] This is why a private state database and a public state database have been created.

The Quorum has made the following changes to the Ethereum Go client in order to work:

- Unlike Ethereum, it is a blockchain that can only operate if the user grants permission for it to do so.
- It is not formed using Proof of Work but rather by using the Raft or Istanbul BFT algorithms for consensus.
- P2P connections can only be established between nodes that the P2P layer has granted authorization.
- Separate databases are preserved for private information and public use in state databases.
- It is now possible to employ the "private transactions" validation algorithm for blocks.
- Transaction processing has been modified so encrypted hashes, rather than transaction data, can be used when sensitive information must be protected.
- Quorum refuted the idea that using gas would add additional costs to a transaction.

2.1. Blockchain

This section will explore the inner workings of Blockchain technology, with a focus on its first implementation in the BitCoin system. The system's security is ensured through digital signatures, which are applied to each BitCoin transaction. Every node in the BitCoin network is responsible for receiving and verifying transactions, which are then added to a public ledger accessible to everyone. The Bitcoin network can reach a consensus on the order of transactions due to each block in the Blockchain containing the previous block's hash. This is illustrated in Figure 2. The proof-of-work consensus process, where a node must solve a difficult mathematical challenge before broadcasting the new Blockchain, allows the network to determine which blocks from various nodes should be combined. This process relies on the abilities of miner nodes, which specialize in solving complex mathematical problems.

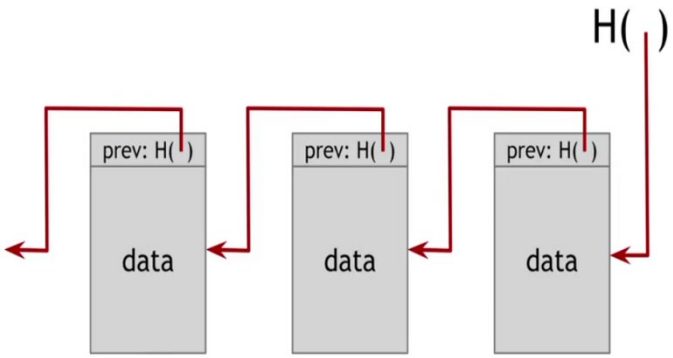

Figure 2. How Blockchain uses the hash function to maintain the order of blocks.

Due to these security measures, the Blockchain is immune to fraudulent transactions. This is because if an attacker were to tamper with even one block on the Blockchain, they would end up altering the entire chain, as each subsequent block is linked to the previous one. After the transaction has been signed, the block is then broadcast throughout the network. Once all nodes have verified the transaction, it can be recorded on the public ledger, finally resulting in the transfer of funds from "A" to "B" [3]. The working of the Blockchain is depicted in Figure 3.

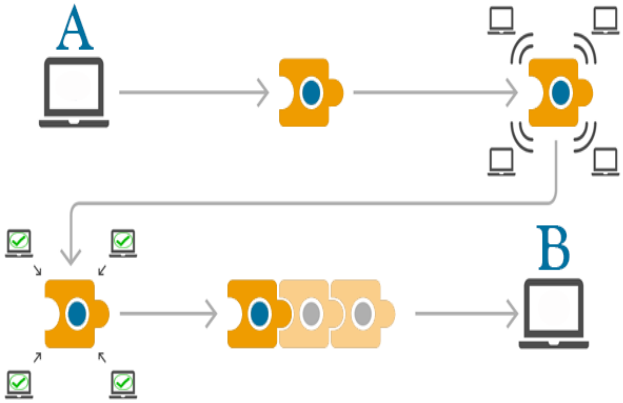

Figure 3. A financial transaction using blockchain technology.

The Blockchain eliminates the risk of double spending in Bitcoin transactions through a consensus mechanism. This mechanism ensures that only the first transaction to solve a mathematical problem is added to the public ledger, while others are rejected. This helps to prevent the same coins from being spent multiple times by a single user. In the event of two blocks with identical hashes, both are rejected by the Blockchain. For further information on how the Blockchain operates, refer to the paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [2].

2.2. Raft consensus algorithm

The Raft algorithm is a consensus algorithm that is used to run a distributed, replicated ledger. In the Raft algorithm, there are three roles that a node can play: leader, follower, or candidate. At any given time, each node is one of these three roles.

In the Raft algorithm, time is divided into fixed-length terms, and terms are numbered with integers. At the start of a new term, one or more candidates try to win the election for

leader. If candidates win the election, they become the leader for the rest of the term. The leader sends heartbeats to followers, and if a follower does not receive a heartbeat from the leader, they become candidates and run for election.

During the term, the leader is responsible for replicating all transactions in the ledger. The leader tells the followers to add a new entry, and once the leader receives a response from most of the followers, the entry is considered committed and written to the ledger. This process is called "replication."

In the Raft algorithm, there are various methods for setting the timeout for the election, including a state transition model that helps prevent multiple nodes from switching from one candidate to another simultaneously. The Raft algorithm ensures that there is always one leader; if a client talks to a follower, the follower will redirect the client to the leader. If a follower does not receive a request from the leader, they will run for election and, if elected, become the next leader.

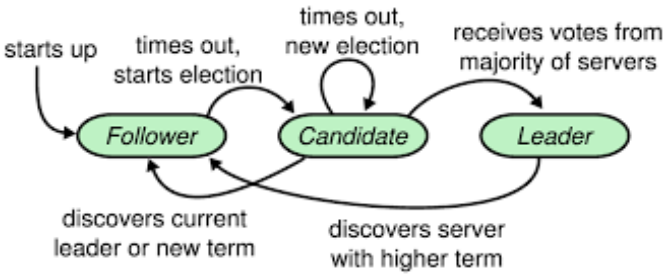

Figure 4. Servers' status in the Raft.

The majority of Raft may be divided into sections known as terms. Every term has its duration and number of years, and each commences with an election in which candidates compete for the new chief executive position. In the event that one of the candidates is victorious in the election, that individual assumes the role of leader.

2.3. Leader Election

In Raft, nodes initially start as followers, and the leader sends heartbeats to verify its own status and prevent its followers from timing out. If a follower has not heard from the leader within the specified timeout period, it will become a candidate and initiate a new election by sending a Request Vote RPC to request votes from other nodes. All nodes in the network then cast their votes, and the node with the most votes is elected as the new leader.

There is a chance that even with a randomized timeout, there may still be a split vote in certain situations. The solution to this problem is to extend the current term, which will provide each node with a new timeout for the next election. An example of what happens in a network with a split vote is depicted in the figure 5.

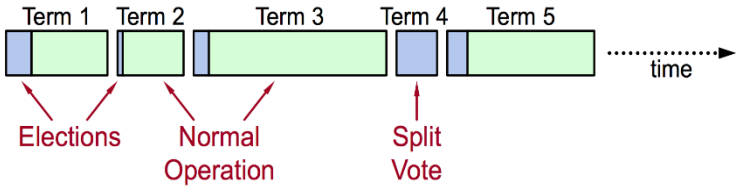

Figure 5. Terms in the Raft.

2.4. 4.2 Log Replication.

The leader is responsible for handling consumer requests and committing them once it receives confirmation from a majority of the nodes in the cluster that the request has been stored. This confirmation is achieved through the leader sending an RPC called Append Entries to the nodes. If the majority of nodes confirm the storage of the request, the leader can then commit the request..

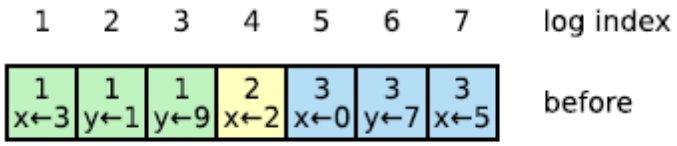

Figure 6. Nodes log in Raft network.

Term numbers, commands, and indexes are shown in Figure 6. Only a unit of time is defined, and the index the logbook.

2.5. Raft on Blockchain

The voting-based consensus technique, such as Raft, requires nodes to be pre-configured and known before they can be utilized. In Raft, the elected leader is responsible for receiving and appending signed blocks from the nodes in the network to the Blockchain. The leader will send Append Entries RPCs, including the Blockchain's highest and lowest committed indices. Once miners solve a new block of transactions, it is broadcasted to all nodes in the network. This requirement for known and configurable nodes differentiates Raft from proof-based consensus algorithms.

In order for "A" to make a transaction with "B," a block is created and signed by "A." The block is then sent to "C" for validation and approval. If the block is deemed valid, it is added to the Blockchain and broadcast through the Append Entries RPC. This allows the transaction to take place with "B." The approval process by "C" results in the block being added to the Blockchain and broadcast for all nodes in the network.

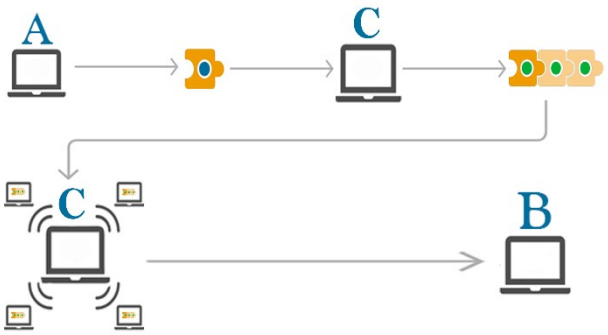

Figure 7. Transaction using the Raft blockchain technology.

In Raft, extra constraints are put in place to ensure that all nodes in the network are in sync with each other. This includes having one person in charge of each level of the hierarchy and ensuring that once a leader has confirmed a transaction, it cannot be altered in any way. Additionally, if the entry word and index of two different logs are the same, the logs are the same up until that index. Furthermore, if one node commits a command in a given

index, all other nodes will do the same. Each block in Raft has a "hash section," where the block's content and a nonce are hashed together. This means that if two blocks have the same hash, the leader will not accept them. The block architecture in Raft is shown in Figure 8.

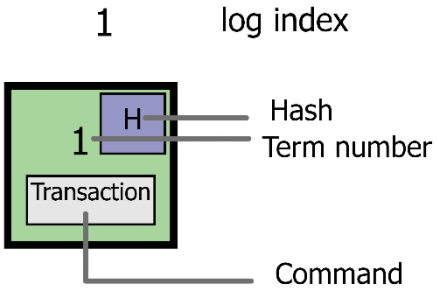

Figure 8. The new block architecture.

Here, algorithms 1 and 2 show how both the follower and the lead roles will work when the Raft is used as the consensus mechanism for Blockchain. Algorithm 3 shows how the network will choose who will be the leader.

Algorithm 1: the role of leader when Blockchain uses Raft as consensus algorithm

```
1.  While(This.State==Leader)
2.  {     RespondToTrans()

4.  {     if (search (trans.hash)) then       RejectTrans();
                Else {      AddTrans();
3.        SendAppenEntriesRPC();//for all
4.              if(isMajority())  then    N=CommitTheTrans()
5.                Else   delete()   }      }
6.        RespondToHeartBeat()
7.          {     if(Last Index>follower.nextIndex)
8.                  {   DecrementNextIndex()
9.                    retry sending();     }        }
10.                 if (N>CommitIndex& MajortyCommit[i]>=N& then      log.term==currentTerm)
11. .                     SetCommitIndex(N);    }
12. StepDownToFollower();
```

When using Raft as the consensus algorithm for the Blockchain, the role of the leader is of utmost importance. As stated earlier, the leader is responsible for processing transactions and adding them to the Blockchain. The steps involved in the leader's response to a transaction request are described in lines 2-5. The leader checks for instances of double spending on the active Blockchain and then performs a binary search. Any transactions with the same hash value are rejected and not broadcast. However, a record of it is maintained on the leader's Blockchain.

It is noted later that leaders may need to step down and inform the new leader about the number of committed indexes for the new leader to keep up with any transactions that

occurred during their absence. This is to ensure that the new leader is up to date with all transactions that took place while the previous leader was unavailable.

Algorithm 2: the role of the Follower when Blockchain uses Raft as a consensus algorithm

```
1.  RespondToRPC
2.  {       if(isVoteRequest()){
3.          If(this.term< term& this.Lastindex< Lastindex) Then  VotPsitive();
4.                  Else   VotNegative();   }//if1
5.                Else if(isAppenEntries()){
6.                if(isLeaderPartOfTrans())   Then   ValidateTrans();
7.                Else        AppendEntry();    }//elseif
8.                 Else if(isAcknowledgement())     {
9.               if(reciveAcknowledgement())  Then  CommitEntre();
10.                 Else        ReSendTransAction();     }//elseif
11.         IssueTransAction(sender I, ReciverId, Segnetur, Data, Hash, TermNum);
    }
```

When the Raft algorithm is used for consensus in a Blockchain system, the role of the followers is crucial. The Raft node communicates with other nodes in the network only through RPCs and only responds when requested. The followers are instructed on how to respond to request vote RPCs in lines 2-4. The request's legitimacy is first checked by examining the term number and most recent index. The Append Entries request is handled in lines 5-7. If the leader is involved in a transaction, the follower will examine it before it is included in the block to be added to the Blockchain. The rest of the code in the algorithm outlines the conditions and timing for completing transactions.

Algorithm3: the election procedure when Blockchain uses Raft as a consensus algorithm

```
1.  If (follower not receiving heart beat)
2.  {    If(electionTimeOut())
3.     {        incrementCurrentTerm();
4.              ChangeToCadidate();
5.              VoteForMyself();
6.               RequestVoteRPC(term, candidateID,
7.              LastLogIndex, LastLogTerm);
8.            While(IsCandidate())
9.            {    WaitForFeedback();
10.  Int x=ProcessFeedBack();
11.                Foreach (EntryIn_AppendEntry())       {
12.                    If(this.Term< entry.term)                  {
13.                          ChangeStateToFollower();   }//if        }//foreach
14.       If(x>(n/2 +1))  {
15.             ChangeStateToLeader();
16.             Send_RPCAppendEntry(); //heartbeat
17.                          }
18.       Else if(x(n/2 +1))    {
19.             ChangeStateToFollower();       }
20.       Else //no one won    {
                    i. incrementTerm();

startNewElection();      }    }//while   }//if2    }//end if1
```

When the current leader cannot perform their duties, an election for a new leader is initiated. During this time, the followers will not receive any communication from the current leader. When a follower turns, it becomes a candidate, increases its term, votes for itself, and requests votes from other nodes in the network. The candidate will then wait for responses and monitor the results to determine if they have won the election. If no leader is elected (if the number of votes received is less than N/2, where N is the number of nodes in the network), the candidate will become the leader and start sending heartbeats.

Factors such as scalability, security, block creation rate, rewards, and node joining policies can significantly impact the usefulness of blockchain technology. A company can achieve its goal of implementing blockchain technology by considering these factors.

3. Fraud Prevention Use Case

Telecom companies are undergoing a digital transformation, incorporating technologies such as virtualization, A.I., RPA, and others. By implementing Blockchain, CSPs can derive numerous benefits and improve their operations while preparing for the future. When roaming to a partner network, the partner network sends CDRs data through an offline method provided by a financial information organization (DCH). The DCH is then responsible for ensuring the transmission of important files to the Home Network. All roaming operator combinations may have to follow a permission-based blockchain.

A network of nodes from each operator confirms every transaction between the home network and the visitor network through a roaming subscriber. The home network of the subscriber is where they originally originate. The VPMN, as per its contract with the HPMN, must send CDR data whenever a subscriber in a heavily used network causes an issue. The digital contract is now active, and its terms are enforceable. As a result, the

VPMN will receive information from the HPMN about the prices supported by the provided services, which the HPMN will then send back to the VPMN. This allows payments based on Blockchain-based smart contracts to be made efficiently and securely while still adhering to the terms of the agreements.

As a result of CSPs getting rid of the DCH as a middleman in the pricing structure, prices may go down for consumers. In a time when trust and safety are very important, blockchain technology has the potential to change complex datasets across multiple parties.

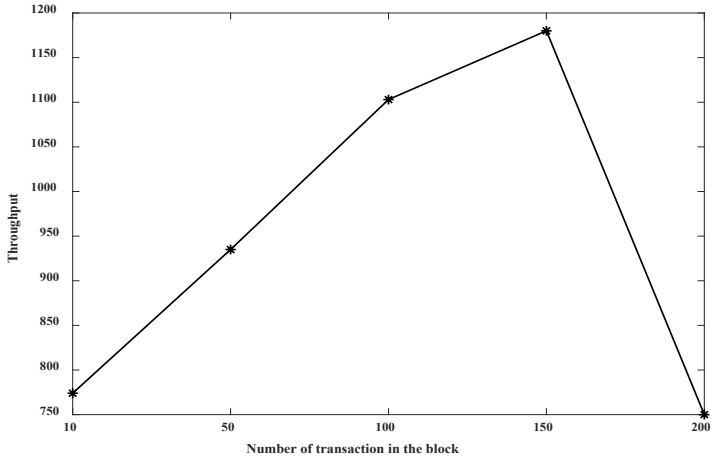

Figure 9. Throughput versus number of transactions in the block

4. Simulator-based model

This section will outline the model for a permissioned blockchain system. In a distributed peer-to-peer network, nodes communicate with each other to verify their conditions. The data is stored in a blockchain, a copy of the state, and written as a chain of blocks linked together through cryptographic hashes. Each block is linked to the previous one through its hash. Transactions, rather than blocks, are secure trades between two parties protected by asymmetric encryption. Blocks are collections of transactions of a fixed size, and miners and buyers are two types of nodes. Miners verify and add blocks of accepted transactions, while customers are the nodes that initiate transactions.

An associate said that every node in the regional network has external powers that could be used as a formal tool for an external evaluation. Customers who buy things are the ones who let the network know about transactions. In the next step, which is putting these parameters into blocks, the status of the chain will then change. Each block is either in a state of compatibility or in a state of waiting so that it does not get rejected. When they agree on something, most miners will go to the block in question. After each transaction has been checked, each participant makes a list of the ones that are still missing. These blocks are then added to the Blockchain in the order shown below. Even though the block and, later, the merged transactions are not added to the Blockchain immediately, much waiting is involved. So, the process of getting the miners to agree on something is used to figure out the next mass that must be followed within the context of the common state of the transactional order. As a general rule, we choose a subset of nodes to be "leaders" and give them the job of quickly suggesting an end to a certain goal. Figure 9 shows one way a blockchain network could be used.

After the jobs in the current block are done, the person who won the election will come up with an idea for a new block. This is something that all nodes in the network can agree on and follow on the Blockchain. It has been decided that the blockchain system will have two different layers. As a result, network miners perform dreadful initial and associate bases, which collect and store transaction blocks provided by buyers. This level is supported by a second layer running the consensus procedure. When these units are linked, transaction execution is provided, and the joint ledger is updated for the gauge, we tend to think about the product, how much time was spent on the transaction, and how well it was done. Because of this, the transactions that are added to the Blockchain make it look like they are happening more slowly than they are. When figuring out trade latency, we often look at how long it has been since the last submission and how committed the block is to the contract.

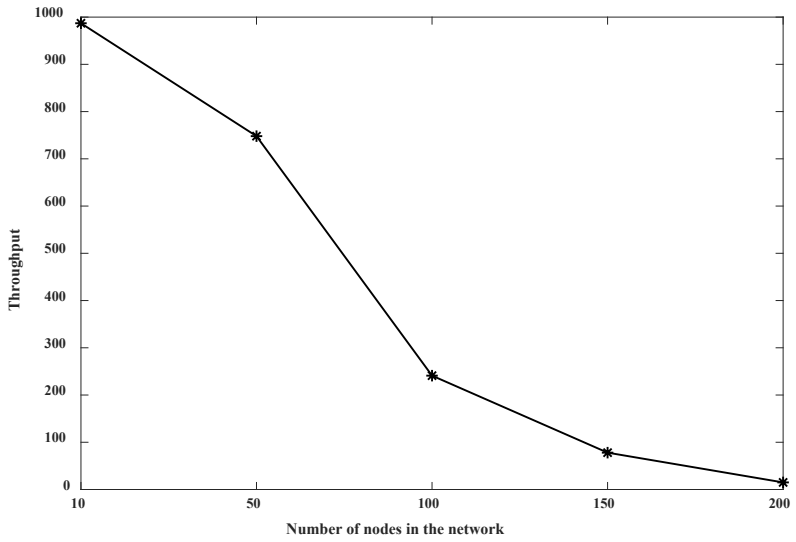

Figure 10. Throughput decreases with a larger number of nodes

5. Conclusion

The private Blockchain, which relies on votes rather than proofs to reach consensus, is the subject of this study rather than the public Blockchain. Raft as a consensus algorithm for Blockchain is discussed in this work, which describes a thorough implementation of the consensus algorithm through three alternative algorithms. In addition, this work describes the Raft as a Bitcoin consensus technique. This research examined the performance and scalability differences between a permissioned and public blockchain and the extent to which Hyperledger material is a viable alternative to existing centralized financial systems. A considerable gain in performance and the ability to measure it can be achieved by sacrificing decentralization by shifting authority and trust outside the network. Confidence in a permissioned blockchain does not require any processing power, unlike the progressive elimination of throughput concerns in public blockchains. The Hyperledger content should be able to meet the needs of the enterprise in circumstances of commercial telecommunications use that a public blockchain cannot. Using the raft consensus has resulted in a decent amount of output, according to the results.

ACKNOWLEDGEMENT This research is funded by the Deanship of Research and Graduate Studies in Zarqa University /Jordan"

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online].
[2] G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618
[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in Proceedings of IEEE Symposium on Security and Privacy (S.P.), San Jose, CA, USA, 2016, pp. 839-858.
[4] B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online].
Available: https://ssrn.com/abstract=2394738
[5] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184-191.
[6] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), Lyon, France, 2015, pp. 490-496.
[7] S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,", Self-published Paper, Aug. 2012. [Online]. Available:
https://peercoin.net/assets/paper/peercoin-paper.pdf
[8] Nxtwiki, "Whitepaper:Nxt,", 2015. [Online]. Available: http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt
[9] A Al-Qerem, A Hamarsheh "" Statistical-Based Heuristic for Scheduling of Independent Tasks in Cloud Computing "". International Journal of Communication Networks and Information Security (IJCNIS) Volume 10, No. 2, 2018, pp. 358-365.
[10] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc.Symposium on Operating Systems Design and Implementation, 1999, pp. 173-186.
[11] L. Lamport, "The Part-Time Parliament," ACM Transactions on Computer Systems, 16(2):133-169, 1998.
[12] M. Zeeshan, S. Khan" A Robust Carrier Frequency Offset Estimation Algorithm in Burst Mode Multicarrier CDMA based Ad Hoc Networks", International Journal of ommunication Networks and Information Security (IJCNIS) Volume 4, No. 3, 2012, pp. 174-181
[13] A. Al-Qerem, M. Alauthman, A. Almomani and B. B. Gupta, "Iot transaction processing through cooperative concurrency control on fog–cloud computing environment," Soft Computing, vol. 24, no. 8, pp. 5695-5711, 2020/04/01 2020.
[14] "Consortium chain development." [Online]. Available: https://github. com/ethereum/wiki/wiki/Consortium-Chain-Development
[15] M. Du, X. Ma, Z. Zhang, X. Wang and Q. Chen, "A review on consensus algorithm of blockchain," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, 2017, pp. 2567-2572.
[16] The ZILLIQA team, "The ZILLIQA Technical Whitepaper,", 2017. [Online]. Available: https://docs.zilliqa.com/whitepaper.pdf
[17] I. Moraru, D. G. Andersen, and M. Kaminsky, "There is more consensus in egalitarian parliaments," In Proc. SOSP'13, ACM Symposium on Operating System Principles (2013), ACM.
[18] M. Du, X. Ma, Z. Zhang, X. Wang and Q. Chen, "A review on consensus algorithm of blockchain," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, 2017, pp. 2567-2572.

Notes on contributors

Prof. Ahmad Alqerem obtained a BSc in 1997 from JUST University and a Master's in computer science from Jordan University in 2002. Ph.D. in mobile computing at Loughborough University, U.K., in 2008. He is interested in concurrency control for mobile computing environments, particularly transaction processing. He has published several papers in various areas of computer science.

Dr. Ala Hamarsheh is an associate professor at the Faculty of Engineering and Information Technology of the Arab American University of Jenin. Dr. Hamarsheh obtained a Ph.D. in engineering sciences from Vrije Universiteit Brussel (VUB)/Brussels-Belgium in 2012. He graduated in computer science at the Faculty of Science, Birzeit University, Palestine, in 2000. He obtained an MSc in computer science at the Kind Abdullah II School for I.T., The University of Jordan, Jordan, in 2003. Dr. Hamarsheh has published numerous papers in international refereed journals and conferences.

Dr. Ali Mohd Ali was born in 1982 in Jordan. Mutah University awarded him a Bachelor of Engineering in Computer Engineering in 2005. In 2013, he received a Master's degree in Computer and Communication Engineering from Universiti Kebangsaan Malaysia (UKM). In 2021, he received a Ph.D. in Computer and Communications Engineering from the University of Huddersfield in the United Kingdom. He is currently an assistant professor of communications and computer engineering at Al-Ahliyya Amman University. His primary research interests are in analyzing communication system reliability using complex modeling techniques and approaches to WLAN optimization.

Yasmeen shaher Alslman

Yasmeen Alslman is currently a Ph.D. Candidate at Princess Sumaya University for Technology.

Dr. Mohammad Alauthman received a Ph.D. from Northumbria University Newcastle, U.K., in 2016. He is currently an Assistant Professor with the Information Security Department at Petra University, Jordan. His research interests include cyber-security, cyber forensics, advanced machine learning, and data science applications.