International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Comparison of Algorithms used in Blockchain-based Mobile Ad Hoc Networks (MANETs)

Dr. Sangheethaa .S[1], Dr. Arun Korath[2]

[1]Associate Professor, Department of Information Technology, University of Fujairah, UAE

[2]Professor and Director, Vedavyasa Institute of Technology, Kerala, India

Abstract: ***Blockchain-based mobile ad hoc networks (MANETs) are gaining popularity in recent years due to their high reliability and secure transactions. In a blockchain-based MANET, nodes are more vulnerable to attacks due to the dynamic nature of the network, which can make it challenging to maintain network security. While Proof of Work (PoW) can be effective in maintaining consensus in a MANET environment, it presents several challenges such as limited resources, network latency, security, energy consumption, and scalability. Byzantine Fault Tolerance (BFT) is a concept in distributed computing that refers to a system's ability to tolerate failures or attacks by nodes that behave maliciously or fail in unexpected ways. In this paper, we discuss the challenges faced in Software-Defined Networking (SDN) in Blockchain MANET. In summary, SDN and BFT are two different approaches to improving the performance, resilience, and security of distributed networks.***

Keywords: MANET, Blockchain, Proof of Work, Proof of Stake, BFT, SDN

1. Introduction

Mobile ad hoc networks (MANETs) are a type of wireless networks that can be formed on-the-go by mobile devices without the need for a pre-existing infrastructure. However, the lack of central control and infrastructure in MANETs make them susceptible to attacks and security breaches. Blockchain technology has been proposed as a solution to enhance the security and privacy of MANETs. In this literature review, we will explore some of the research studies that have investigated the use of blockchain technology in MANETs.

Blockchain-based secure mobile ad hoc network (BSMAN) for the Internet of Things (IoT) uses a consensus mechanism to ensure the integrity of transactions and a smart contract to manage network resources. The authors demonstrate the effectiveness of their proposed solution through simulation experiments [1].Blockchain-based authentication and authorization mechanism for MANETs uses smart contracts to verify the identities of nodes and to manage access control policies [2]. Blockchain-based trust management framework for MANETsuses smart contracts to manage trust between nodes and to ensure the integrity of transactions[3]. Blockchain-based security framework uses smart contracts to manage access control policies, to authenticate nodes, and to ensure the integrity of transactions [4].

2. Proof of Work (PoW)

The Proof of Work (PoW) algorithm is a consensus mechanism used in blockchain-based MANETs to validate transactions and create new blocks in the chain. The PoW algorithm requires nodes in the network to compete to solve a cryptographic puzzle, which involves finding a hash value that meets a specific requirement.

In a MANET, nodes that want to create a new block must first solve the puzzle, which involves making multiple attempts at finding the correct hash value. This process requires significant computational power, which means that nodes that have more resources (such as processing power, memory, and energy) are more likely to solve the puzzle and create a new block.

Once a node solves the puzzle, it broadcasts the solution to the rest of the network, along with the new block of transactions it has validated. Other nodes in the network can then verify the solution and the new block, and if they are correct, they can add the new block to their copy of the blockchain.

The difficulty of the puzzle can be adjusted dynamically to maintain a stable rate of block creation and prevent malicious nodes from taking over the network. This is done by changing the requirements for the hash value, such as requiring more leading zeros in the hash or increasing the size of the hash space.

The PoW algorithm in MANETs is designed to ensure that nodes in the network cannot create new blocks or manipulate transactions without performing the required computational work. This makes it more difficult for malicious nodes to attack the network and ensures that the network remains secure and decentralized. However, the PoW algorithm can also be energy-intensive, which can be a challenge in MANETs where energy efficiency is a critical factor.

Challenges in using PoW algorithm in Blockchain Manet

Using the Proof of Work (PoW) algorithm in a blockchain-based MANET can present several challenges, some of which are specific to the mobile ad hoc network environment. Here are some of the key challenges that can arise:

1) **Limited resources:** In a MANET, nodes have limited resources such as processing power, memory, and battery life. The PoW algorithm requires a significant amount of computational power to solve the

cryptographic puzzles, which can be a challenge for nodes with limited resources.

2) **Network latency:** In a MANET, nodes can move around, connect and disconnect from the network, and the topology can change rapidly. This can result in increased network latency, which can impact the time it takes to reach consensus in the network.
3) **Security:** The PoW algorithm is designed to be secure against attacks, but it is not completely immune to all forms of attacks. In a MANET, nodes are more vulnerable to attacks due to the dynamic nature of the network, which can make it challenging to maintain network security.
4) **Energy consumption:** PoW requires a lot of energy to solve the cryptographic puzzles. In a MANET, where nodes are often battery-powered and energy is a scarce resource, this can be a significant challenge. The high energy consumption of PoW can also contribute to environmental concerns.
5) **Scalability:** The PoW algorithm can also present scalability challenges in a MANET. As the number of nodes in the network increases, the computational and energy requirements to maintain consensus also increase, making it more difficult for new nodes to join the network.

In summary, while the PoW algorithm can be effective in maintaining consensus in a blockchain-based MANET, it presents several challenges such as limited resources, network latency, security, energy consumption, and scalability. These challenges need to be carefully considered and addressed when designing and implementing blockchain-based MANET systems that use the PoW algorithm.

Proof of Stake (PoS)

The Proof of Stake (PoS) algorithm is a consensus mechanism used in blockchain-based MANETs to validate transactions and create new blocks in the chain. In contrast to the Proof of Work (PoW) algorithm, which requires nodes to perform computational work to validate transactions, the PoS algorithm chooses nodes to validate transactions based on the number of coins or tokens they hold.

In a PoS-based MANET, nodes that want to create a new block must first stake a certain amount of their coins or tokens as collateral. This collateral is used to ensure that the nodes have a vested interest in maintaining the network and validating transactions honestly.

Once a node has staked its collateral, it is eligible to validate transactions and create new blocks in the chain. The node is chosen to validate transactions based on the amount of collateral it has staked. For example, if a node has staked 10% of the total number of coins or tokens in the network, it will be chosen to validate 10% of the transactions.

If a node validates transactions correctly, it is rewarded with new coins or tokens. If it validates transactions incorrectly or behaves maliciously, its collateral is confiscated, and it may be banned from the network.

The PoS algorithm is less energy-intensive than PoW and can be more suitable for MANETs, where energy efficiency is a critical factor. However, the PoS algorithm also has its own challenges, such as the potential for centralization, where nodes with large amounts of collateral have more power and influence over the network. To mitigate this risk, some PoS-based MANETs use techniques like random selection of validators and limiting the amount of collateral a node can stake.

Challenges in using PoS algorithm in Block Chain Manet

Proof of Stake (PoS) is a consensus algorithm that is gaining popularity in blockchain-based MANETs due to its energy efficiency and low computational requirements compared to Proof of Work (PoW). However, PoS also presents some unique challenges in the MANET environment. Here are some of the key challenges:

1) **Centralization:** PoS consensus is based on the concept of staking, where nodes are required to put up a certain amount of cryptocurrency as collateral to participate in the consensus process. This can lead to centralization, as nodes with more resources can stake more and potentially have a greater influence on the consensus process.
2) **Security:** In a PoS-based MANET, nodes that have more stake (i.e., more cryptocurrency) have more power in the consensus process. This can create a security risk if a large number of nodes are controlled by a single entity or a small group of entities.
3) **Network fragmentation:** In a PoS-based MANET, nodes that have more stake are often given more responsibility in the network. This can create network fragmentation if there is a large imbalance in stake distribution, with certain nodes having a disproportionate amount of influence.
4) **Sybil attacks:** Sybil attacks occur when an attacker creates multiple fake identities (i.e., nodes) to gain control of the network. In a PoS-based MANET, the attacker can create multiple identities by acquiring a small amount of cryptocurrency and using it to stake multiple nodes.
5) **Stakeholder participation:** In a PoS-based MANET, stakeholder participation is critical for maintaining network security and integrity. However, there may be challenges in incentivizing stakeholders to participate in the network, especially if there is a lack of clear rewards or penalties for participation or non-participation.

In summary, while PoS is a promising consensus algorithm for blockchain-based MANETs, it presents several challenges such as centralization, security, network fragmentation, sybil attacks, and stakeholder participation. These challenges need to be carefully considered and addressed when designing and implementing blockchain-based MANET systems that use the PoS algorithm.

Byzantine Fault Tolerance (BFT)

Byzantine Fault Tolerance (BFT) is a concept in distributed computing that refers to a system's ability to tolerate failures or attacks by nodes that behave maliciously or fail in unexpected ways. In a BFT system, nodes can agree on a course of action even if some nodes in the network are compromised or behaving maliciously.

In a BFT system, each node has a copy of the same data, and nodes communicate with each other to reach a consensus on the state of the system. The nodes exchange messages with each other and agree on a decision if a certain threshold of nodes reach the same conclusion.

To achieve BFT in a MANET, nodes can use techniques like digital signatures and cryptographic hash functions to verify the authenticity of messages and prevent attacks like double-spending and Sybil attacks. BFT algorithms are designed to ensure that nodes can reach a consensus even if a certain number of nodes in the network are compromised or behaving maliciously.

One example of a BFT algorithm is the Practical Byzantine Fault Tolerance (PBFT) algorithm. In PBFT, nodes exchange messages with each other to validate transactions and reach a consensus on the state of the system. The algorithm requires a certain number of nodes to reach agreement on a decision before it is accepted, which makes it resistant to attacks by malicious nodes.

BFT is an important concept in blockchain-based MANETs, as it enables nodes to reach a consensus on the state of the system and prevent attacks by malicious nodes. By ensuring that the network can tolerate failures or attacks, BFT makes the network more secure and reliable.

Challenges in Byzantine Fault Tolerance (BFT) in BlockchainManet

Byzantine Fault Tolerance (BFT) is a consensus algorithm that is designed to be resilient to arbitrary faults or attacks, making it an attractive choice for blockchain-based MANETs. However, using BFT in a MANET environment can present several challenges, including:

1) **Message delay and loss:** In a MANET, messages can experience delay or loss due to network congestion, interference, or node mobility. This can lead to inconsistencies in the consensus process, as nodes may receive different sets of messages or receive them at different times.
2) **Node churn:** In a MANET, nodes can join and leave the network frequently due to node mobility or battery depletion. This can make it challenging to maintain a stable set of nodes for the consensus process, and can increase the risk of message delay or loss.
3) **Scalability:** BFT consensus requires a significant amount of communication overhead and computational resources, which can make it challenging to scale the network as the number of nodes increases. This can lead to higher latency and slower transaction processing times.
4) **Faulty nodes:** BFT is designed to be resilient to faulty nodes, but it relies on the assumption that the majority of nodes are honest and behave correctly. In a MANET environment, it can be more difficult to distinguish between faulty and malicious nodes, which can make it challenging to maintain network integrity.
5) **Security assumptions:** BFT relies on certain security assumptions, such as the assumption that a certain number of nodes are honest and non-colluding. In a MANET environment, these assumptions may not hold true, which can make it challenging to maintain network security and integrity.

In a nutshell, while BFT is a promising consensus algorithm for blockchain-based MANETs, it presents several challenges such as message delay and loss, node churn, scalability, faulty nodes, and security assumptions. These challenges need to be carefully considered and addressed when designing and implementing blockchain-based MANET systems that use the BFT algorithm.

Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is an approach to network architecture that separates the control plane from the data plane, enabling centralized control of network devices and making it easier to manage and configure networks. In MANETs, SDN can be used to enable greater flexibility and control over the network, even in the absence of a fixed infrastructure.

In a traditional MANET, each node communicates with neighboring nodes and routes traffic based on local decisions. This approach can lead to suboptimal routing and congestion, as well as difficulty in managing and configuring the network.

In an SDN-based MANET, the control plane is separated from the data plane, and network devices are managed centrally by a controller. The controller communicates with the network devices and provides instructions on how to forward traffic and manage network resources. This approach enables more intelligent routing decisions, load balancing, and greater control over network traffic.

SDN in MANETs can also enable more dynamic and flexible network configuration, as the controller can adjust routing policies and network resources in real-time based on changing network conditions. This makes it easier to manage and configure the network, even in the absence of a fixed infrastructure.

One approach to implementing SDN in MANETs is to use a hybrid architecture, where some nodes in the network act as controllers and communicate with neighboring nodes to manage the network. This approach can provide greater scalability and resilience, as multiple nodes can act as controllers and work together to manage the network.

Overall, SDN in MANETs can provide greater flexibility, control, and manageability over the network, enabling more intelligent routing and dynamic network configuration. This can lead to better network performance, greater resilience, and improved network security.

Challenges faced in Software-Defined Networking (SDN) in BlockchainManet

Software-Defined Networking (SDN) is a networking architecture that allows for programmable and centralized network management, making it an attractive choice for blockchain-based MANETs. However, using SDN in a MANET environment can present several challenges, including:

1) **Resource constraints:** MANETs are typically resource-constrained environments, with limited bandwidth, processing power, and battery life. This can make it challenging to implement SDN controllers or switches that require significant computational resources.
2) **Mobility and topology changes:** MANETs are highly dynamic environments, with nodes that are mobile and topology that can change rapidly. This can make it challenging to maintain stable network paths or to manage network policies, as nodes may join or leave the network or change their positions frequently.
3) **Security:** SDN architectures rely on a centralized controller to manage network policies and routing, making it a single point of failure and a potential target for attackers. In a blockchain-based MANET, maintaining network security and integrity is critical, and SDN architectures need to be designed to be resilient to attacks.
4) **Interoperability:** Interoperability between different SDN controllers or switches can be challenging, particularly in a MANET environment where nodes may use different hardware or software platforms.
5) **Scalability:** SDN architectures can be challenging to scale, particularly in a MANET environment where the number of nodes can change rapidly and network resources are limited.

In summary, while SDN is a promising networking architecture for blockchain-based MANETs, it presents several challenges such as resource constraints, mobility and topology changes, security, interoperability, and scalability. These challenges need to be carefully considered and addressed when designing and implementing blockchain-based MANET systems that use SDN architectures.

Comparison of Proof of Work (PoW) vs Proof of Stake (PoS)

Proof of Work (PoW) and Proof of Stake (PoS) are two popular consensus algorithms used in blockchain-based systems, including MANETs. Both PoW and PoS serve the same purpose of verifying transactions and achieving consensus in a distributed network. However, they differ in their approach to achieving this goal.

Here are some key differences between PoW and PoS:

1) **Resource Requirements:** PoW requires nodes to perform complex computational puzzles to validate transactions and create new blocks in the chain, which requires significant computational resources and energy consumption. In contrast, PoS requires nodes to hold a certain amount of cryptocurrency as collateral to participate in the consensus process, which consumes far less energy.
2) **Security:** PoW is considered highly secure since it requires a significant amount of computational power to manipulate the network. PoS is also secure but relies on the assumption that nodes holding a large amount of cryptocurrency have an incentive to act in the best interest of the network.
3) **Decentralization:** PoW is more decentralized since anyone can participate in the consensus process by investing in computational resources. PoS is less decentralized since it favors nodes with a large amount of cryptocurrency, which can lead to centralization.
4) **Scalability:** PoW is often criticized for its scalability issues since it requires a significant amount of computational resources to validate transactions. In contrast, PoS is more scalable since it consumes less energy and can process more transactions.
5) **Environmental Impact:** PoW is highly energy-intensive and contributes significantly to carbon emissions. PoS, on the other hand, consumes significantly less energy, making it a more environmentally friendly alternative.

In summary, PoW and PoS have their own advantages and disadvantages. PoW is highly secure but consumes significant computational resources, while PoS is more energy-efficient but may lead to centralization. Ultimately, the choice between PoW and PoS depends on the specific needs and goals of the network.

Comparison of Software-Defined Networking (SDN) And Byzantine Fault Tolerance (BFT)

Software-Defined Networking (SDN) and Byzantine Fault Tolerance (BFT) are two different approaches to improving the performance, resilience, and security of distributed networks.

Here are some key differences between SDN and BFT:

1) **Focus:** SDN focuses on separating the control plane from the data plane, enabling centralized management and control of network devices. BFT, on the other hand, focuses on achieving consensus and fault tolerance in distributed networks by tolerating arbitrary failures, including Byzantine failures.
2) **Goal:** The goal of SDN is to provide greater flexibility, control, and manageability over the network, enabling more intelligent routing and dynamic network configuration. The goal of BFT is to provide fault tolerance and consensus in distributed systems even when some nodes are malicious or fail.
3) **Implementation:** SDN is implemented through a centralized controller that manages the network devices, whereas BFT is implemented through distributed consensus algorithms that allow nodes to reach agreement on the state of the network.
4) **Tradeoffs:** SDN often sacrifices some level of decentralization for greater control and management over the network. BFT, on the other hand, often sacrifices some level of performance and efficiency for greater fault tolerance and security.
5) **Applicability:** SDN is applicable to a wide range of networks, including traditional wired networks, wireless networks, and MANETs. BFT, on the other hand, is specifically designed for distributed systems, including blockchain-based systems, and may not be suitable for other types of networks.

In summary, SDN and BFT are two different approaches to improving the performance, resilience, and security of distributed networks. SDN focuses on centralized management and control of network devices, while BFT focuses on achieving consensus and fault tolerance in distributed systems. The choice between SDN and BFT depends on the specific needs and goals of the network.

The choice of consensus algorithm or networking approach to be used in a MANET depends on the specific requirements, constraints, and goals of the network. Each algorithm or approach has its own advantages and disadvantages, and the best one will depend on the specific use case. Here are some considerations to keep in mind:

1) **Security:** If security is the top priority, then Byzantine Fault Tolerance (BFT) may be the best option. BFT is specifically designed to tolerate Byzantine failures, including malicious or faulty nodes.
2) **Energy efficiency**: If energy efficiency is a concern, then Proof of Stake (PoS) may be a good option. PoS requires significantly less computational power and energy consumption compared to Proof of Work (PoW).
3) **Scalability:** If scalability is a priority, then Software-Defined Networking (SDN) may be the best option. SDN allows for greater flexibility, control, and manageability over the network, enabling more intelligent routing and dynamic network configuration.
4) **Decentralization**: If decentralization is a priority, then PoW may be the best option. PoW allows anyone to participate in the consensus process by investing in computational resources, making it more decentralized.
5) **Application:** The specific application of the MANET will also influence the choice of algorithm or approach. For example, if the MANET is being used for blockchain-based transactions, then PoW or PoS may be the best option.

In summary, there is no one-size-fits-all solution when it comes to choosing the best algorithm or approach for a MANET. The choice will depend on the specific requirements, constraints, and goals of the network. It is important to carefully evaluate each option and choose the one that best meets the needs of the application.

References

[1] "A Blockchain-Based Secure Mobile Ad Hoc Network for the Internet of Things" by J. Huang, et al. (2019)
[2] "A Blockchain-based Authentication and Authorization Mechanism for Mobile Ad Hoc Networks" by S. Ali, et al. (2020)
[3] "A Blockchain-Based Trust Management Framework for Mobile Ad Hoc Networks" by M. Raza, et al. (2018)
[4] "Blockchain-Based Security Framework for Mobile Ad Hoc Networks" by A. Alharbi, et al. (2018).

References

Dr. Sangheethaa S has completed her PhD from Anna University, India in Information and communication Engineering in the year 2012. She has completed ME in Network and Internet Engineering from Karunya University, India and BE in Information Technology from Bharathiyar University India. Her area of interest is Mobile ad hoc networks, security in mobile networks and recently her research area is in Blockchain. Currently she is working as Associate professor in the College of Information Technology, University of Fujairah, Fujairah, United Arab Emirates.

Dr. Arun Korath has completed his PhD in Management science from Anna University Chennai, India in 2013. He completed Master of Business Administration from Kannur University, India and BE in Information Technology from Bharathiyar university. His area of interest is in Systems, ERP management. Currently he is the Director of Vedavyasa institute of Technology, Malappuram, India.