Hindawi
Security and Communication Networks
Volume 2021, Article ID 8363131, 12 pages
https://doi.org/10.1155/2021/8363131

Research Article

Blockchain Network Propagation Mechanism Based on P4P Architecture

Junjie Huang,[1] Liang Tan,[1] Sun Mao,[1] and Keping Yu[2]

[1]*College of Computer Science, Sichuan Normal University, Chengdu, China*
[2]*Global Information and Telecommunication Institute, Waseda University, Tokyo, Japan*

Correspondence should be addressed to Sun Mao; sunmao@sicnu.edu.cn

Received 29 May 2021; Revised 6 July 2021; Accepted 26 July 2021; Published 5 August 2021

Academic Editor: Qingqi Pei

Blockchain is a mainstream technology in which many untrustworthy nodes work together to maintain a distributed ledger with advantages such as decentralization, traceability, and tamper-proof. The network layer communication mechanism in its architecture is the core of the networking method, message propagation, and data verification among blockchain nodes, which is the basis to ensure blockchain's performance and key features. When blocks are propagated in peer-to-peer (P2P) networks with gossip protocol, the high propagation delay of the protocol itself reduces the propagation speed of the blocks, which is prone to the chain forking phenomenon and causes double payment attacks. To accelerate the propagation speed and reduce the fork probability, this paper proposes a blockchain network propagation mechanism based on proactive network provider participation for P2P (P4P) architecture. This mechanism first obtains the information of network topology and link status in a region based on the internet service provider (ISP), then it calculates the shortest path and link overhead of peer nodes using P4P technology, prioritizes the nodes with good local bandwidth conditions for transmission, realizes the optimization of node connections, improves the quality of service (QoS) and quality of experience (QoE) of blockchain networks, and enables blockchain nodes to exchange blocks and transactions through the secure propagation path. Simulation experiments show that the proposed propagation mechanism outperforms the original propagation mechanism of the blockchain network in terms of system overhead, rate of data success transmission, routing hops, and propagation delay.

1. Introduction

Blockchain is a decentralized infrastructure that uses a cryptographic chained block structure to verify and store data, uses distributed node consensus algorithms to generate and update data, and uses smart contracts to program and manipulate data and is now widely used in finance, agriculture, healthcare, charity, and the Internet of Things [1–4]. The technical architecture of blockchain mainly consists of data layer, network layer, consensus layer, and application layer. Among them, the data layer includes the underlying data blocks and their chain structure (the block structure is shown in Figure 1), supported by hash algorithms, Merkle trees, and other related technologies to protect the integrity and traceability of block data. The network layer includes data propagation mechanisms and transaction verification mechanisms, supported by peer-to-peer (P2P) network technologies to complete the transmission and verification of data among distributed nodes. The consensus layer includes various consensus mechanisms to achieve data consistency among distributed nodes through various consensus algorithms. The application layer can realize various application scenarios of blockchain and the realization of related systems [5].

As with edge computing [6], Blockchain has received wide attention from academia and industry. Its core technology as a digital cryptocurrency can solve the double payment problem that digital currencies have long faced. In general, there are two forms of double payment attacks [7, 8]. One is that the attacker uses a single amount to deal with multiple objects at the same time. If these objects complete the transactions without being recorded in the legitimate blockchain, the attacker achieves double-spending. Although only one legitimate transaction will be

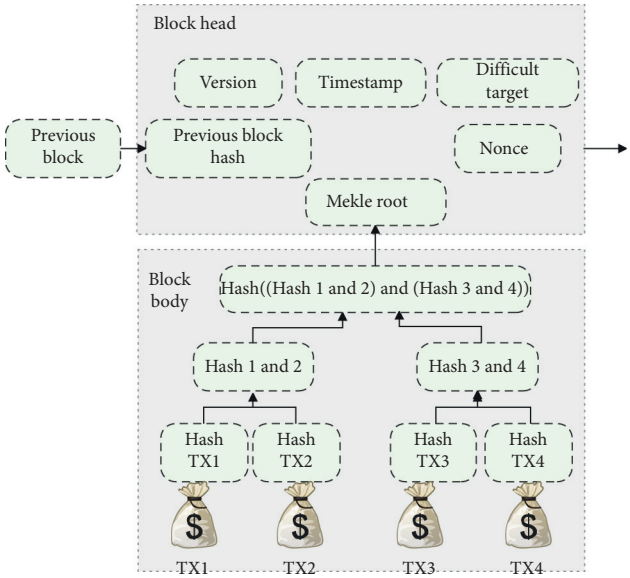

Figure 1: Block structure.

recorded in the chain among multiple transactions, the attacker has already benefited from it. Second, the attacker uses his own powerful computing power to launch a double-spending attack. After the first transaction is completed and recorded in the blockchain, the attacker uses his strong computing power to record the second transaction in the private blockchain and continues to mine the private chain until a legitimate and longer chain is mined to replace the previous public chain so that the second transaction is also confirmed and double consumption is completed. The literature [9] gave a scenario of blockchain forking, as shown in Figure 2. At a certain point, if the length of the blockchain is L and the block at the end of the chain is C, the miner Jack calculates the difficulty value by arithmetic power, first digs the block D, and starts to propagate D to the whole network. At the same time, another miner in the system, Tomas, is also mining a blockchain of length L. It coincides that Tomas mines a block D' alone before D reaches him. He does not know that block D has been mined and starts to spread D' to the whole network. As these two blocks are continuously broadcast, the nodes in the system will maintain two chains of the same length $L+1$, Chain_Jack and Chain_Tomas, centered on Jack and Tomas, which form a fork.

The literature [10] pointed out that blockchain network forks mainly originate from the propagation delay of blocks or transactions, i.e., the slow propagation speed of blocks or transactions and the high probability of network forks. To reduce the fork probability and improve the propagation speed of the blockchain network, this paper proposes a blockchain network propagation mechanism based on the P4P architecture, i.e., Blockchain_P4P. iTracker server in the P4P architecture is used to provide policy guidance to the blockchain nodes, namely, iTracker calculates the p distance and virtual cost between nodes and provides the IP address of the node with the closest distance and lowest virtual cost to the requesting node. Therefore, the blockchain propagation mechanism based on P4P architecture can effectively

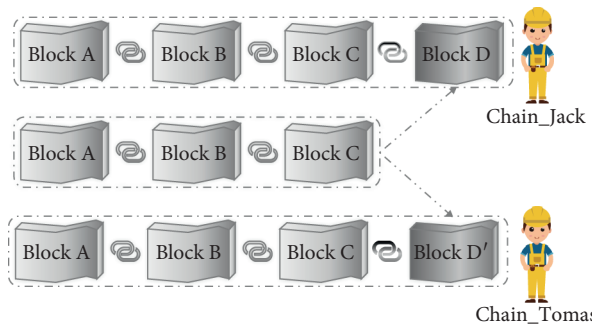

Figure 2: Blockchain network fork situation.

improve the network transmission efficiency and accelerate the speed of propagation.

The main contributions of this paper are summarized as follows.

(1) To reduce the probability of blockchain forking due to propagation delay, this paper focuses on optimizing the propagation path of blocks. For the first time, P4P technology is integrated with the network layer of the blockchain, and the efficient communication efficiency of P4P is used to optimize the propagation mechanism of the blockchain and improve the performance of the blockchain network.

(2) We first propose Blockchain_P4P, a P4P-based blockchain network architecture, and introduce in detail how to optimize the blockchain network layer using P4P technology. Then, we propose the Blockchain_P4P path propagation mechanism and formalize the Blockchain_P4P propagation mechanism through algorithms and timing diagrams.

(3) We use delay-tolerant network (DTN) simulator to simulate the process of nodes routing data. The gossip propagation mechanism is simulated using Random + Epidemic routing algorithm, and Blockchain_P4P propagation mechanism is simulated using Dijkstra + Prophet algorithm. Through the simulation, it is concluded that the Blockchain_P4P propagation mechanism outperforms the gossip mechanism in terms of propagation delay, data transmission success rate, and routing overhead, while the number of routing hops is higher than the gossip mechanism.

The remainder of this paper is organized as follows. Section 1 summarizes the optimization method of the fork problem. Section 2 is the preparatory knowledge. Section 3 is the blockchain network architecture and algorithm based on P4P. Section 4 is the characteristics of the propagation mechanism and gossip protocol in this paper. Section 5 shows the simulation experiments of the two propagation mechanisms. Section 6 gives the conclusion.

2. Related Work

In recent years, in order to reduce the probability of chain forks, academia and industry have conducted in-depth research on this. The current common methods to reduce chain

forks include two. One is to optimize the transmission protocol of the block, and the other is to increase the transmission rate of the block or reduce the propagation time of the block. First of all, for the propagation protocol of the blockchain, the gossip protocol is mainly used to broadcast blocks or transactions. Figure 3 shows the propagation process of a block or transaction [11]. As shown in the figure, the initiator of a block or transaction first checks and verifies the difficulty of the block or transaction and then transmits the transaction and block through the gossip protocol. The transmission process requires the initiator to send an inv message to the receiver. The receiver uses the inv message to determine whether the block or transaction already exists locally. If the receiver does not store the block or transaction locally, the receiver will send getdata information to the initiator. Finally, the initiator sends the block or transaction to the receiver to complete the transmission of the block data. In the process of node interaction, the network latency mainly comes from the difficulty check of the sender and the hash verification of the block as well as the delay in the transmission of inv messages, getdata messages, and blocks or transactions between the sender and the receiver. In order to optimize the protocol of blocks and reduce the propagation delay, it was proposed in the literature [10–12] that single-node optimization and pipelining of the propagation to reduce the propagation delay of blockchain networks, respectively. Among them, single-node optimization stipulates that the sender performs difficulty checking on the block, and the receiver performs hash verification on the block. The streamlining of the propagation process is to pass the block difficulty check and block hash verification to the receiver. Although these optimization schemes reduce the propagation delay to a certain extent, they also bring about other security problems and also affect the performance of the blockchain network, and the effect of reducing the total network propagation delay is not obvious.

Second, for improving the block propagation speed, a random mining group selection technique is proposed in the literature [13] to improve the block propagation speed to reduce the probability of successful double-spending attacks, and it is experimentally demonstrated that the probability of an attacker finding the next block is less than 50% when the number of mining groups is greater than or equal to 2. However, this random mining group technique has extra cost consumption, while the effect of reducing double-spending attack is less desirable. The literature [14] discussed the relationship between block propagation delay and blockchain fork probability, as shown in formula (1). P_b denotes the probability of mining out a block. t is a time variable that represents the range of time variation of block propagation. $f(t)$ denotes the percentage of blocks that are received by nodes after propagation at time t. After analyzing the formula, we could conclude that the higher the probability of P_b or the slower the block propagation will increase the probability of block forking:

$$P_{\text{fork}} \approx P_b * \int_0^{\infty} (1 - f(t)) d_t. \tag{1}$$

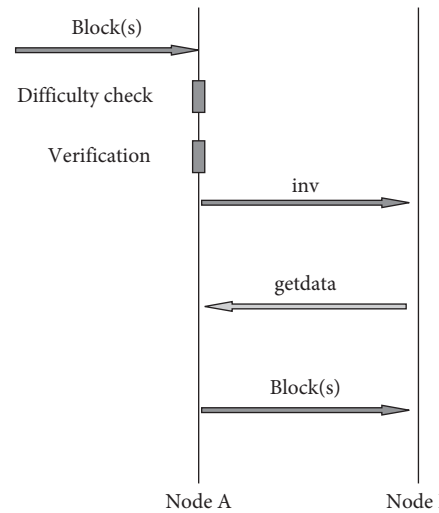

Figure 3: Process of block or transaction transfer.

The literature [15] investigated the performance of block propagation in a P2P network similar to Bitcoin, and by simulating the P2P network, it is shown that the block propagation delay is mainly affected by the average round-trip time. When the average round-trip time is longer, the probability of forking occurring is higher. The literature [16] summarized the relationship between blockchain throughput and forking rate and proposes "Fastchain," which aims to improve the throughput of blockchain systems by reducing the block propagation time and gives a formula for the block generation rate as shown in equation (2). Among them, the forking rate is the probability of discarding blocks per second, and the effective block rate is the probability of adding blocks to the longest chain per second:

$$\text{Block rate} = \text{forking rate} + \text{effective block rate}. \tag{2}$$

A theoretical analysis of resistance to 51% attack versus prevention of double flower attack was presented by Sarwar et al. [17, 18]. Since 51% attacks can lead to double payment attacks on blockchain networks, five advanced protection techniques and their limitations have been proposed by Sarwar et al. for 51% attacks, but this is for theoretical discussion only. The literature [19–21] accelerated the propagation speed of blockchain networks by changing the topology of nodes, but it reduces the QoS of the network and increases the propagation delay when there is congestion in the network. The literature [22] proposed the Ari protocol to replace the gossip protocol for blockchain networks, aiming to optimize the propagation protocol for the P2P layer, which makes the block propagation a crossnet instead of a one-way tree, thus achieving a reduction in block propagation time. However, this protocol consumes more network bandwidth and has an impact on the performance of the blockchain network. The literature [23] proposed a most trusted chain confirmation mechanism to defend against fork attacks and thus enhance blockchain security. However, this mechanism does not sufficiently consider the network link situation. The literature [24] proposed a probabilistic

verification scheme PvScheme, which can effectively reduce block propagation delay and improve blockchain network performance after comparison experiments, but the scheme does not consider the QoS of the network comprehensively. The literature [25] pointed out the phenomenon of forking in blockchain-based IoT. Jameel et al. used a deep learning approach to increase the transmission rate, which reduces the transmission delay, minimizes the probability of forking, and avoids excessive overhead to large-scale IoT networks. The literature [26] proposed a strategy to accelerate block propagation and reduce the probability of chain forking, namely, PiChu. The strategy propagates and verifies blocks by parallelism and demonstrates experimentally the feasibility and efficiency of the strategy. The literature [27] evaluated and surveyed existing blockchain simulators, then designed a novel blockchain simulator, and studied the effect of network latency on blockchain forks using different mining difficulties. The literature [28] investigated the phenomenon of temporary forking of blockchain, then proposed a mathematical model to describe the effect of arithmetic competition of mining pools on temporary forking from the perspective of miners, and proved the feasibility of the model through experiments. The literature [29] proposed a new framework for using wireless mobile miners (MMs) for computation in blockchain networks, based on which the architecture was analyzed to show that the latency required for movement and the high latency generated by wireless connections may cause a fork. Finally, it is experimentally demonstrated that using lower transmission power and reducing the movement of each MM can reduce the forking probability. The literature [30] proposed a P4P improvement scheme based on distributed tracker, aiming to improve the transmission rate of peer nodes through improving routing efficiency. This literature pointed out that iTracker's description of resource download paths is mainly rated by the weights of different paths, and the calculation of path weights mainly contains three constraints of delay, bandwidth, and cross-domain communication cost. Formula (3) gives the communication cost weighting function $C(l_{i,j})$ for links $l_{i,j}$, where the constant C denotes the cross-domain communication cost, $f(l_{i,j}, T)$ is the delay consumption function, T denotes the delay demand constraint of the service request, $f(l_{i,j}, B)$ is the bandwidth consumption function of link $l_{i,j}$, and B denotes the bandwidth demand constraint of the service request:

$$C\left(l_{i,j}\right) = C + f\left(l_{i,j}, T\right) + f\left(l_{i,j}, B\right). \tag{3}$$

A weighted graph is created based on the link communication cost weighting function $C(l_{i,j})$, and the best path is selected to achieve communication in combination with the Dijkstra algorithm.

In summary, the methods to reduce the probability of block forking mainly include two aspects. First, the propagation delay of the network is reduced by optimizing the propagation protocol of blocks, which in turn reduces the forking rate. Although the block propagation delay is reduced to a certain extent, it also brings other security problems, such as DDOS attacks. Moreover, the optimization of block propagation protocols does not reduce the total propagation delay of blocks. Second, by increasing the propagation speed of blocks, however, the above literature does not fully consider the blockchain network load, QoS, and bandwidth capacity, also brings other security issues, and increases the network overhead. Therefore, the above solutions are not comprehensive enough in reducing blockchain network forking.

3. Preparatory Knowledge

3.1. P4P Architecture. This section first introduces the concepts and important components of P4P and then illustrates the communication process between the important components of P4P and ISP.

P4P is a lightweight application-based framework, which mainly opens an explicit communication interface between P2P applications and network operators, and peer nodes can call the communication interface to get network information and improve the performance of P2P applications. P4P generally consists of the control plane, data plane, and management plane. Among them, the management plane is to monitor the behavior of the control plane. The data plane is to distinguish the application flow and set the priority of the application flow, which may not be needed. The control plane is the core component of P4P, which introduces the iTracker server and provides the interface to communicate with ISPs, including the policy interface, the capability interface, and the P4P distance interface [31], as shown in Figure 4. Among them, the policy interface mainly provides network policies for peer nodes, such as which links should be avoided when the network is congested. The capability interface allows peer nodes to request resources or capabilities from iTracker. The P4P distance interface provides the internal view seen by iTracker and the external attempt seen by P2P applications. The internal view is the network topology $G = (V, E)$, V is the set of nodes, E is the set of links, and the nodes in the V sets are also called PID nodes, which are mainly used to represent network topology information. The external view is a fully connected mesh network, and the external view is given visible PID-*i* and PID-*j*. iTracker will calculate the distance P_{ij} of two nodes based on the internal distance and route of the network, which is usually calculated based on open shortest path first (OSPF) weights or border gateway protocol (BGP) priority. In addition, iTracker will also calculate the virtual cost for different links and select the lowest virtual cost with the shortest P_{ij} as the connection path for peer nodes [32].

3.2. Gossip Protocol. This section introduces the concepts related to the gossip protocol and the advantages and disadvantages of using this protocol for data exchange.

Gossip protocol is a decentralized protocol, which is used as a core technology in P2P networks to synchronize data among nodes in a distributed system. Figure 5 shows the process of transmitting information by the gossip protocol. The core idea of the protocol is that a node of the system passively receives data sent from other nodes, and then actively propagates the updated state to its neighbor nodes after completing

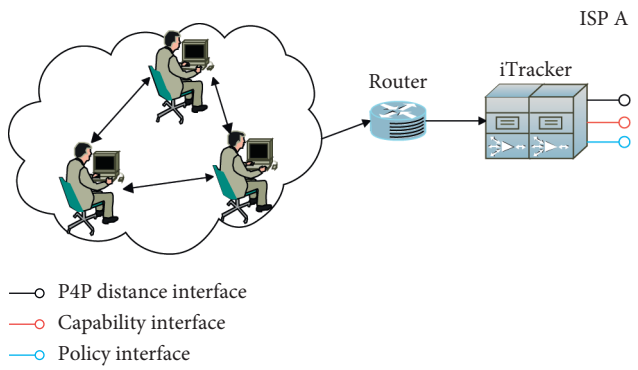

Figure 4: P4P architecture.

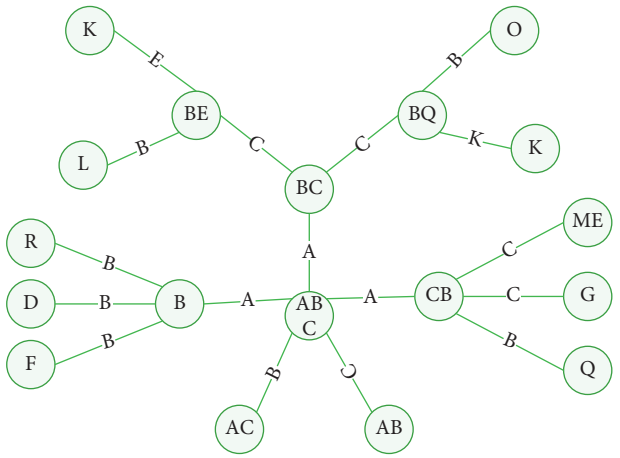

Figure 5: Gossip protocol propagation process.

local updates, at which time the neighbor nodes complete passive updates. If a node still has not updated its local data after a period of time, it will actively send requests to neighboring nodes and then complete active updates. When the nodes of the distributed system have been updated several times, the information of the rest of the nodes in the system is finally stored locally, so the gossip protocol ensures the ultimate consistency of the distributed system and does not affect other nodes even if there is a single point of failure, making the whole system more fault-tolerant [33]. In Bitcoin, blockchain nodes use the gossip protocol to broadcast blocks or transactions to their neighboring nodes, and then, neighboring nodes that receive blocks or transactions continue to broadcast in this way until all nodes in the system receive blocks or transactions, thus completing the dissemination of information. However, this protocol suffers from high propagation delay and can seriously affect the reliability and security of block and transaction transmission when there are link failures and congestion in the network. Therefore, although the gossip protocol can ensure the consistency of data across nodes, it also affects the blockchain network performance.

3.3. Blockchain Architecture. This section introduces the architecture of blockchain, briefly analyzes the role of each layer in the architecture, and points out the focus of the research work in this paper.

Blockchain acts as a distributed database ledger, and each node follows a set of communication protocols to achieve synchronization of ledger data. The blockchain architecture is given in Figure 6. As shown in the figure, the blockchain mainly consists of the data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. The data layer encapsulates the data block, hash function, timestamp, and other technologies. The network layer defines the P2P network and data propagation mechanism. The consensus layer encapsulates a variety of consensus algorithms, such as PoW and PoS. The incentive encapsulates the issuance mechanism and dispensing mechanism of economic incentives. The contract layer encapsulates the script code, algorithm mechanism, etc. The application layer encapsulates various application scenarios of blockchain [34]. In the blockchain architecture, the network layer is the core layer, and the propagation mechanism encapsulated in this layer is the key to ensure the secure transmission of blocks or transactions. Therefore, in order to speed up block propagation, this paper uses P4P technology to improve the transmission efficiency of the blockchain network.

4. P4P-Based Blockchain Network Propagation Mechanism

In order to accelerate the propagation delay of blocks or transactions, this paper proposed a blockchain network propagation path mechanism based on the P4P architecture. The core idea is that when a blockchain node performs distance and link cost calculations and returns the best node to the source node before establishing a connection with other nodes and transmitting blocks or transactions. In particular, this routing approach takes into account the network condition, routing overhead, and link cost consumption and minimizes the network propagation delay. In order to describe the P4P-based blockchain network propagation mechanism more clearly, we proposed the P4P-based blockchain network architecture, Blockchain_P4P and Blockchain_P4P propagation mechanism, in the following subsections.

4.1. P4P-Based Blockchain Network Architecture Blockchain_P4P. This section introduces a P4P-based blockchain network architecture Blockchain_P4P, points out the components of the architecture diagram, analyzes the features of the architecture, and demonstrates that the application of P4P technology can effectively improve network performance and speed up data transmission.

P4P is a technology proposed to prevent excessive consumption of network bandwidth. It can make full use of the advantages of network operators and network service providers (ISPs) to provide P2P nodes with network topology, bandwidth, and link cost information, and according to the information provided, it optimizes the QoS and transmission efficiency of the P2P network, which not only reduces the network load but also improves the P2P network performance. The blockchain is a P2P network presented in a flat star-like structure with a

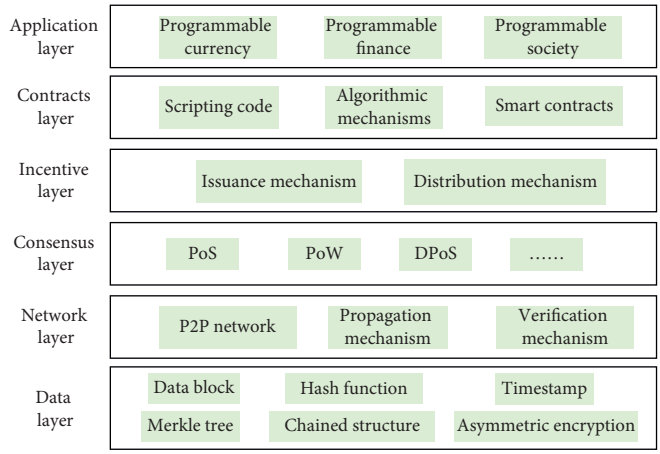

Figure 6: Blockchain architecture model.

communication mechanism of Gossip protocol. If the blockchain nodes are transmitting blocks or transactions, there is a link failure or network congestion and other conditions will inevitably lead to a higher propagation delay, which will affect the performance of the blockchain network. Therefore, using P4P technology to reduce network load, optimize node transmission efficiency, and improve the characteristics of node propagation speed, a P4P-based blockchain network architecture Blockchain_P4P is proposed, as shown in Figure 7. Figure 7 shows the iTracker deployed by ISPs in three different regions, each of which contains blockchain nodes and routers. In an autonomous system, the iTracker server is deployed by a network service provider and can provide blockchain nodes with network topology, virtual cost calculation, network inbound and outbound traffic ratio, and other information. Based on this information, iTracker will select the node set with low link consumption and fast transmission rate to return to the blockchain node, and the blockchain node will forward the block or transaction with this set of nodes.

In blockchain networks, the propagation speed of blocks or transactions is affected by the link-state, network state, QoS, and other factors. The P4P technology has the functions of relieving the pressure of Internet transmission, reducing operation cost, and optimizing node connection, which can intelligently provide better connection guidance for blockchain nodes. This guidance is reflected in iTracker's ability to select the most suitable node and return based on the shortest P distance and lowest link consumption. In summary, the P4P technology solves the problem of blockchain nodes' delay in receiving blocks or transactions by other blockchain nodes due to link failures and other reasons on the transmission path, speeds up the propagation speed of blockchain networks and the reliability of node connections, and also improves the transmission performance of blockchain networks.

4.2. Blockchain_P4P Propagation Mechanism. This section focuses on the Blockchain_P4P propagation mechanism, which is formalized mainly through algorithms and sequence diagrams.

The Blockchain_P4P propagation mechanism combines P4P and blockchain technology to speed up the data propagation and improve the reliability of transmission. Algorithm 1 is the Blockchain_P4P algorithm. This algorithm defines the blockchain node set, number of nodes, distance set, IP, BandWidth, and As number. Before a blockchain node sends a request to the iTracker server, it first needs to send the IP, BandWidth, and AsId of the node to the iTracker server to facilitate the node that provides the connection to the blockchain node. Then, iTracker constructs an internal view $G = (V, E)$ based on the network topology information provided by ISP, V is the set of nodes, E is the set of links, the nodes in V are defined as PIDs, and the distance between nodes is expressed as P distance. iTracker performs the calculation of P distance between nodes and link virtual cost based on the internal view and the related network information. Generally, iTracker uses OSPF weights or BGP priority to calculate virtual cost. After the calculation, iTracker selects the blockchain node suitable for connection and returns it to the requesting node. Finally, the requesting node establishes a connection with it.

The following are the definition and description of the relevant interfaces in Algorithm 1.

(i) **Compute (BlockNodeSet, DistanceSet):** the interface input is BlockNodeSet and DistanceSet, which means iTracker calculates the shortest distance of all nodes in BlockNodeSet based on the network topology information provided by ISP, and after the calculation is completed, it returns the shortest path set.

(ii) **chooseNode (BlockNodeSet, shortestPathSet):** the interface input is BlockNodeSet and shortestPathSet, which means iTracker selects the IP of the requesting node to the nearest destination node based on the shortest path set and returns it to the requesting node.

Figure 8 shows the sequence diagram of blockchain nodes requesting iTracker and establishing connections with other nodes. The specific connection flow is as follows:

(1) Blockchain node initiates a request to iTracker.

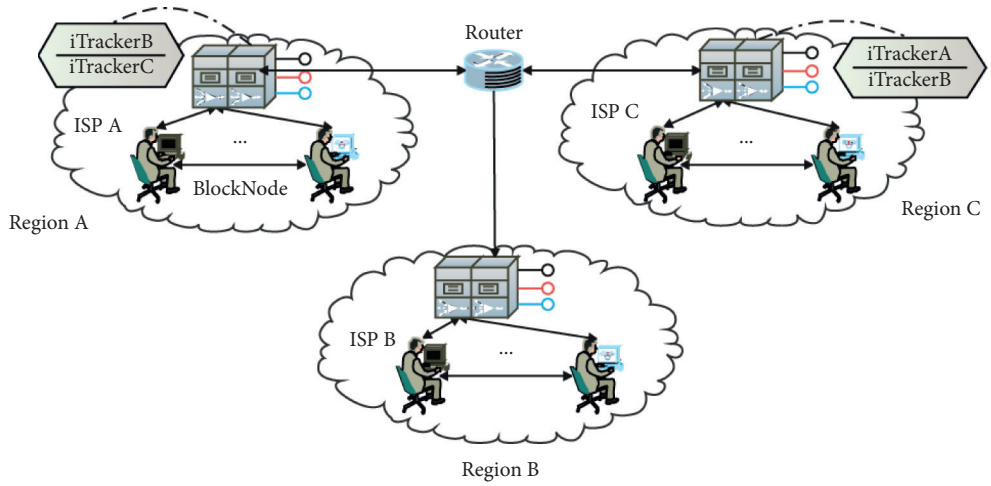

Figure 7: Blockchain network architecture based on P4P.

Input: Num, BlockNodeSet, DistanceSet, IP, BandWidth, AsId
Output: IP_{dst}
(1) NodeSet = ∅
(2) //Add node information to iTracker
(3) **for** each $i \in [1, \text{Num}]$ **do**
(4) $BlockNodeSet \Leftarrow IP_i$
(5) $BlockNodeSet \Leftarrow BandWidth_i$
(6) $BlockNodeSet \Leftarrow AsId_i$
(7) **end for**
(8) //iTracker calculates node distances
(9) shortestPathSet = compute (BlockNodeSet, DistanceSet)
(10) IP_{dst} = choose (BlockNodeSet, shortestPathSet)

Algorithm 1: Blockchain_P4P propagation mechanism.

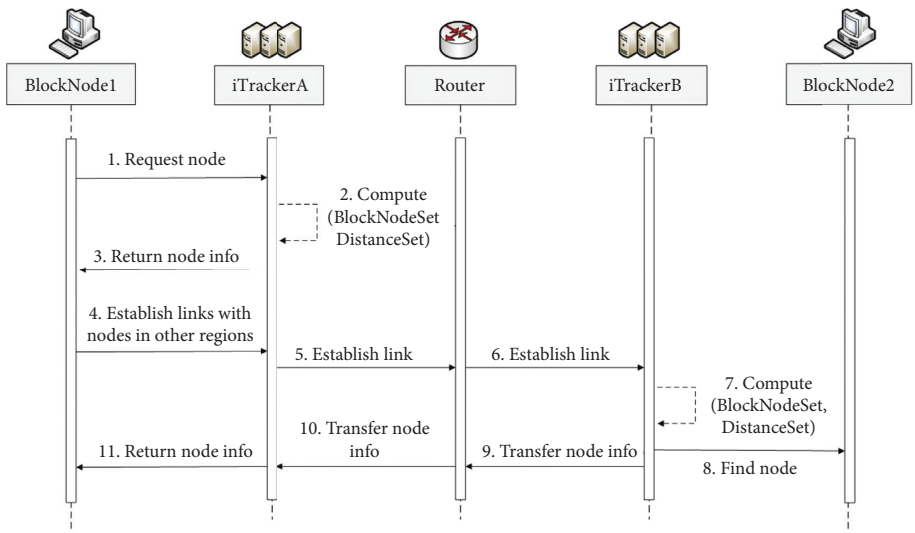

Figure 8: Blockchain nodes establish connections via iTracker to other nodes.

(2) iTracker performs P distance and virtual cost calculation based on the network information provided by ISP. If the best node is found, the IP of the node is returned to the requesting node.

(3) Each iTracker records the IPs of other regional iTrackers, and nodes in different regions can establish connections through the router. When a blockchain node initiates a connection request, the iTracker queries the IP of neighboring iTracker and establishes a connection with it.

(4) After the neighboring iTracker receives the request, it performs P distance and virtual cost calculation.

(5) After the calculation is completed, it transmits the information of the nodes in the region to the source iTracker through the router. When the source iTracker obtains the information of the node, it provides the information to the requesting node.

(6) The requesting node establishes a connection based on the node information provided by the iTracker.

5. Characteristic Analysis

This section provides a detailed analysis of the reliability and security of Blockchain_P4P propagation mechanism and gossip propagation mechanism during block transmission.

P4P technology mainly solves the problem of uncontrollable traffic on the Internet and is also commonly used to optimize the performance of P2P applications. For blockchain, P4P technology improves the propagation delay in the network, greatly reduces the probability of double payment attacks, and better protects the data integrity of blocks and transactions. In Bitcoin and Hyperledger Fabric, the propagation mechanism of blockchain follows the gossip mechanism, which is the basis of blockchain node consensus and is the core of ensuring data consistency of nodes.

In terms of the reliability of block and transaction transmission, the Blockchain_P4P-based propagation mechanism is more reliable than the gossip propagation mechanism because the gossip protocol relies on the network QoS and link quality, and if the network QoS decreases or the link fails, it will not only cause some nodes in the network to fail to receive blocks or transactions for a long time but also increase the total propagation delay. On the contrary, the P4P architecture relies on ISPs to collect network information, allowing ISPs to provide the underlying network state and policy information to P2P applications, which intelligently select data exchange objects based on the policy information. Therefore, when blockchain nodes send blocks or transactions, the capability interface provided by the P4P architecture for blockchain networks is used to request policy guidance from iTracker in priority. iTracker calculates the virtual cost and the P distance between blockchain nodes and then intelligently selects the nodes suitable for blockchain nodes to connect, thus avoiding blockchain nodes from failing to blockchain nodes cannot forward blocks and transactions to neighboring nodes smoothly due to link failure. Therefore, the propagation mechanism based on Blockchain_P4P is more reliable than the gossip propagation mechanism.

As far as the security of transmission is concerned, in Bitcoin, if there is network congestion, it will reduce the propagation speed of blocks and transactions, thus increasing the probability of forking, which gives attackers the opportunity to perform double payment attacks and also puts the security of the blockchain network at risk. In P4P, the iTracker server deployed by ISPs to collect network information calculates the P distance and virtual cost between blockchain nodes based on the network information. iTracker provides the best connection guidance for blockchain nodes based on the calculation results, which avoids blockchain nodes from sending blocks or transactions with nodes that have link failures and saves transmission time. Thus, the propagation mechanism based on Blockchain_P4P improves the speed of block and transaction propagation, reduces the probability of forking, optimizes the blockchain network performance, and guarantees the security of the blockchain network.

In summary, integrating P4P technology into the blockchain network to improve the routing of blockchain nodes and optimize the connection between blockchain nodes not only enhances the reliability and security of the network but also improves the efficiency and QoS of blockchain network communication.

6. Experimental Results

6.1. Experiment Environment. This section introduces the simulator and the experimental environment for the experiments and explains the corresponding performance indicators.

This experiment selects the DTN simulator the ONE V1.6 to simulate Blockchain_P4P, a blockchain network propagation mechanism based on P4P architecture. The running environment is Win10, Intel core i7-5500u CPU ∗ 4 2.40 GHz, memory is 8 GB, and the compilation software is eclipse. The ONE is a simulation platform developed for the DTN environment, which provides a variety of routing protocols and movement models to simulate a more realistic network environment [35, 36]. Figure 9 shows the simulation scenario of the experiment, which contains the blockchain node, ISP, and iTracker. To verify whether the blockchain network propagation mechanism based on the P4P architecture can optimize the latency problem caused by the gossip mechanism and reduce the forking rate, four performance metrics are proposed to evaluate the two propagation mechanisms.

(1) **Latency:** latency is an important metric for blockchain network performance measurement, which consists of two main components. One is the propagation delay of transactions or blocks; the other is the delay of difficulty checking and hash verification of blocks.

(2) **System overhead:** system overhead can measure the memory and CPU resource usage by the operating system. The two propagation mechanisms we

Figure 9: Simulation scenario of the experiment.

simulate consume different amounts of memory and CPU, and this metric measures which propagation mechanism can optimize connections while reducing system overhead.

(3) **Route hops:** the number of routing hops is the number of packets that pass through the router when they are transmitted. If blocks are routed faster and with fewer routing hops, blocks and transactions will be transmitted to neighboring nodes faster.

(4) **Message transmission success rate:** the message transmission success rate is the probability that a packet is successfully routed to the destination node within a specified time. In the experiment, we set the TTL value for each packet, and if the packet is not transmitted to the destination node within a certain time frame, the packet will be lost due to TTL timeout, and if the node transmits the message fast enough, the packet will not be lost due to TTL value timeout, reflecting the strength of the two propagation mechanisms for block and transaction transmission.

6.2. Routing Algorithm Selection for Two Propagation Mechanisms. This section briefly analyzes the characteristics of the gossip and Blockchain_P4P mechanisms and selects different routing algorithms for simulation based on the analyzed characteristics.

The idea of the propagation mechanism of gossip is that neighboring nodes send each other the information that has not been received by each other and then finish the local update; after a period of time, all the nodes in the whole network have received each other's information and the message is consistent. And, the core idea of an epidemic algorithm is that when the initiating node sends a data request to a neighboring node, it first sends a summary vector, and based on the summary vector, it determines whether the other party has already received that data, and if not, it will exchange data with the other party. Like the gossip protocol, the epidemic routing algorithm also forwards data based on replicas. Therefore, we use an epidemic routing algorithm and a random move model to simulate the gossip propagation mechanism in our experiments.

This proposal uses P4P technology to optimize the propagation mechanism of the blockchain network layer, changing from the initial source node sending blocks to neighboring nodes to the source node sending requests to the iTracker server first. iTracker, through route calculation, derives the node with the lowest link consumption and shortest path to the source node, connects with it, and exchanges block data. It can be concluded that iTracker can improve the efficiency of data transmission and avoid a lot of route consumption. Therefore, we chose the Prophet routing algorithm [37] in the simulator to simulate the propagation mechanism based on the P4P architecture. In addition, the P distance is usually selected using the shortest path algorithm, and the closer the distance, the shorter the P distance, so we use the Dijkstra + Prophet algorithm to simulate the propagation mechanism of the blockchain network based on the P4P architecture in the simulation experiment.

6.3. Simulation Comparison of Two Transmission Mechanisms. This section simulates the gossip mechanism and Blockchain_P4P mechanism in terms of four performance metrics, such as routing hops, propagation delay, rate of message transmission success, and system overhead, and provides a brief overview of the simulation results.

After simulating the gossip propagation mechanism and the blockchain network propagation mechanism based on the P4P architecture, the performance metrics such as the number of routes, average delay, transmission success rate, and system overhead under the two propagation mechanisms are derived. We set 100 ~ 600 groups of nodes in 12 h to simulate these two propagation mechanisms, and the comparison of four performance metrics under the two propagation mechanisms is given in Figures 10–13. Figure 10 shows the comparison of the routing hops of the two propagation mechanisms. Since the epidemic algorithm is to forward packets to the encountering node whenever it encounters a node, some nodes may save the same packets and stop exchanging packets when this occurs, and after simulation, the routing hop count of this algorithm is basically maintained at about one hop. For the routing algorithm simulated in this scheme, the number of routing hops is in the range of 2 to 6. This is because the forwarding path of the block data is provided by iTracker, and the forwarding path may face a high number of hops. However, even if the number of hops is high and the quality of the link is good, there will be no link congestion as in the epidemic algorithm.

Figure 11 shows the average latency comparison between the two propagation mechanisms; as shown, the average latency under the gossip propagation mechanism simulated by epidemic is higher than the propagation mechanism of the blockchain network based on the P4P architecture simulated by Prophet. Since the epidemic algorithm is to exchange packets whenever a node is encountered, when there are more nodes in the network and the routes are far away, congestion and high propagation delay are likely to occur. The Prophet algorithm is an efficient routing algorithm that calculates the shortest path to the destination node by the shortest path algorithm, so the propagation delay of this algorithm is lower than the epidemic algorithm.

Figure 12 shows the comparison of the message transmission success rate of the two propagation mechanisms. From the figure, it can be seen that the message transmission success rate of the gossip propagation mechanism simulated

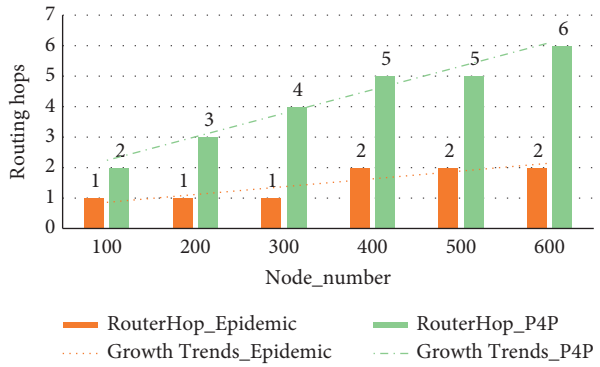

Figure 10: Comparison of routing hops for the two propagation mechanisms.

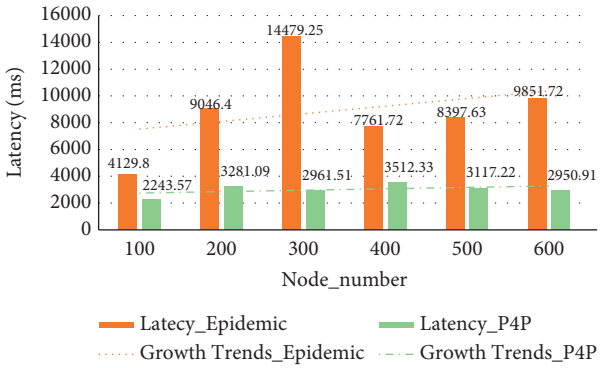

Figure 11: Latency comparison of two propagation mechanisms.

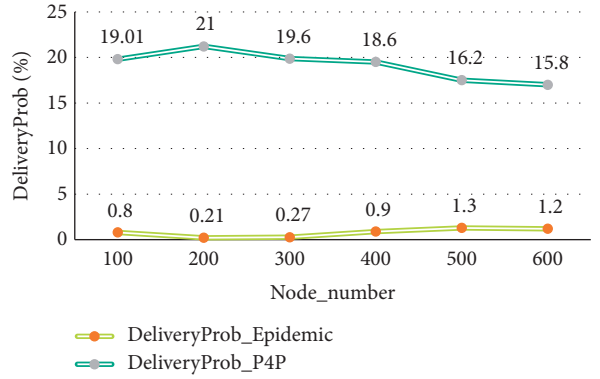

Figure 12: Comparison of the delivery rates of the two propagation mechanisms.

by epidemic is much lower than that of the blockchain network propagation mechanism based on the P4P architecture simulated by Prophet. This is because epidemic has a large number of replicas in the network, and these replica messages are not forwarded in time due to network congestion and exceed the set TTL value resulting in packet drops, thus leading to a lower message transmission success rate.

Figure 13 shows the system overheads of the two propagation mechanisms. The epidemic algorithm is based on a flooding strategy, exchanging packets with the encountered nodes each time, which will bring a high system

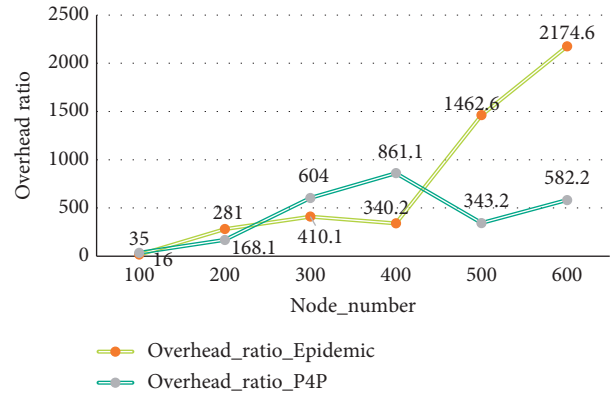

Figure 13: Comparison of the overhead ratios of the two propagation mechanisms.

overhead to the whole system. The Prophet algorithm, on the other hand, selects the nodes on the shortest path to forward packets, which brings less system overhead. As can be seen from the figure, when the node size increases, the system overhead brought by the epidemic algorithm will gradually increase and eventually far exceed that of Prophet.

7. Conclusion

This paper discussed the problem that blockchain networks were highly prone to bifurcation. We first summarized the causes of bifurcation and then gave an optimization scheme to cope with bifurcation. To speed up block propagation, we proposed Blockchain_P4P, a blockchain network propagation mechanism based on P4P, which combined with P4P technology to improve the communication efficiency of blockchain nodes. Through simulation comparison, it was found that the Blockchain_P4P mechanism needs to go through multihop routes when communicating with nodes in other regions, so its routing hop count was higher than that of the gossip mechanism. And, the Blockchain_P4P mechanism outperforms the gossip mechanism in terms of propagation delay, message transmission success rate, and system overhead, which also demonstrated that the proposed Blockchain_P4P mechanism could effectively accelerate the block propagation speed and enhance the network propagation efficiency.

Data Availability

The data of this experiment are all originated from THE ONE simulator, and the packet transmission is simulated by multiple groups of experimental nodes at different time periods, and the REPORT module of the simulator automatically evaluates the latency, routing hops, system overhead, and rate of message transmission success metrics at that time period, and finally, we draw an experimental graph and perform data analysis based on the evaluated data.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant no. 61373162, Sichuan Provincial Science and Technology Department Project under Grant no. 2019YFG0183, and Sichuan Provincial Key Laboratory Project under Grant no. KJ201402.

References

[1] J. Feng, F. Richard Yu, Q. Pei, X. Chu, J. Du, and L. Zhu, "Cooperative computation offloading and resource allocation for blockchain-enabled mobile-edge computing: a deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6214–6228, 2020.

[2] L. Liu, J. Feng, Q. Pei et al., "Blockchain-enabled secure data sharing scheme in mobile-edge computing: an asynchronous advantage actor-critic learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2342–2353, 2021.

[3] L. Tan, H. Xiao, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered crowdsourcing system for 5G-enabled smart cities," *Computer Standards & Interfaces*, vol. 76, Article ID 103517, 2021.

[4] K.-P. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 2021, Article ID 3049141, 1 page, 2021.

[5] N. Shi, L. Tan, W. Li, X. Qi, and K. Yu, "A blockchain-empowered AAA scheme in the large-scale HetNet," *Digital Communications and Networks*, vol. 2020, 2020.

[6] S. Mao, J. Wu, L. Liu, D. Lan, and A. Taherkordi, "Energy-efficient cooperative communication and computation for wireless powered mobile-edge computing," *IEEE Systems Journal*, vol. 2020, Article ID 3020474, 12 pages, 2020.

[7] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava, and P. Chatterjee, "Efficient and privacy-preserving medical research support platform against COVID-19: a blockchain-based approach," *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 111–120, 2021.

[8] C. Pérez-Solà, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Double-spending prevention for Bitcoin zero-confirmation transactions," *International Journal of Information Security*, vol. 18, no. 4, pp. 451–463, 2019.

[9] W. Jian and C. Gongliang, "Bitcoin blockchain bifurcation research," *Communications Technology*, vol. 51, no. 1, pp. 149–155, 2018.

[10] H. Zhu Jianming, "Blockchain network optimal propagation path and incentive combined propagation mechanism," *Computer Research and Development*, vol. 56, no. 6, pp. 1205–1218, 2019.

[11] Y. Shahsavari, K. Zhang, and C. Talhi, "Performance modeling and analysis of the bitcoin inventory protocol," in *Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*, pp. 79–88, Newark, CA, USA, April 2019.

[12] Y. Shahsavari, K. Zhang, and C. Talhi, "A theoretical model for fork analysis in the Bitcoin network," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 237–244, Atlanta, GA, USA, July 2019.

[13] J. Bae and H. Lim, "Random mining group selection to prevent 51% attacks on Bitcoin," in *Proceedings of the 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pp. 81-82, Luxembourg City, June 2018.

[14] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *Proceedings of the IEEE P2P 2013 Proceedings*, Trento, Italy, September 2013.

[15] V. B. Misic, J. Misic, and X. Chang, "On forks and fork characteristics in a bitcoin-like distribution network," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 212–219, Atlanta, GA, USA, July 2019.

[16] K. Wang and H. S. Kim, "FastChain: scaling blockchain system with informed neighbor selection," in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 376–383, Atlanta, GA, USA, July 2019.

[17] S. Sarwar and M.-G. Hector, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, vol. 9, Article ID 1788, 2019.

[18] K. Nicolas, Y. Wang, and G. C. Giakos, "Comprehensive overview of selfish mining and double spending attack countermeasures," in *Proceedings of the 2019 IEEE 40th Sarnoff Symposium*, pp. 1–6, Newark, NJ, USA, September 2019.

[19] M. Sallal, "A bitcoin model for evaluation of clustering to improve propagation delay in bitcoin network," in *Proceedings of the 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES)*, pp. 468–475, Paris, France, August 2016.

[20] M. Owenson, M. Adda, and A. Mo, "Locality based approach to improve propagation delay on the bitcoin peer-to-peer network," in *Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Lisbon, Portugal, May 2017.

[21] M. F. sallal, G. Owenson, and M. Adda, "Proximity awareness approach to enhance propagation delay on the bitcoin peer-to-peer network," in *Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pp. 2411–2416, Atlanta, GA, USA, June 2017.

[22] X. Yang and L. Shi, "Ari: a P2P optimization for blockchain systems," in *Proceedings of the 2019 17th International Conference on Privacy, Security and Trust (PST)*, pp. 1–6, Fredericton, NB, Canada, August 2019.

[23] K. Wang, Y. Wang, and Z. Ji, "Defending blockchain forking attack by delaying MTC confirmation," *IEEE Access*, vol. 8, pp. 113847–113859, 2020.

[24] B. Liu, Y. Qin, and X. Chu, "Reducing forks in the blockchain via probabilistic verification," in *Proceedings of the 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW)*, pp. 13–18, Macao, China, April 2019.

[25] F. Jameel, M. Nabeel, M. A. Jamshed, and R. Jäntti, "Minimizing forking in blockchain-based IoT networks," in *Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, Dublin, Ireland, June 2020.

[26] K. Ayinala, B.-Y. Choi, and S. Song, "PiChu: accelerating block broadcasting in blockchain networks with pipelining and chunking," in *Proceedings of the 2020 IEEE International Conference on Blockchain (Blockchain)*, pp. 221–228, Rhodes Island, Greece, November 2020.

[27] L. Alsahan, N. Lasla, and M. Abdallah, "Local bitcoin network simulator for performance evaluation using lightweight virtualization," in *Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 355–360, Doha, Qatar, February 2020.

[28] C. Chen, X. Chen, J. Yu, W. Wu, and D. Wu, "Impact of temporary fork on the evolution of mining pools in blockchain networks: an evolutionary game analysis," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 400–418, 2021.

[29] G. Lee, J. Park, W. Saad, and M. Bennis, "Performance analysis of blockchain systems with wireless mobile miners," *IEEE Networking Letters*, vol. 2, no. 3, pp. 111–115, 2020.

[30] W. Feng and Li Lixin, "Improved design scheme of P4P based on distributed tracker," *Computer Engineering and Design*, vol. 37, no. 5, pp. 1134–1139, 2016.

[31] H. Xie, Y. R. Yang, A. Krishnamurthy, Y. G. Liu, and A. Silberschatz, "P4p," *ACM SIGCOMM - Computer Communication Review*, vol. 38, no. 4, pp. 351–362, 2008.

[32] Q. Liu, *Research and Implementation of P4P-based Streaming Media on Demand System*, Nanjing University of Posts and Telecommunications, Nanjing, China, 2012.

[33] Z. Shi-jiang, C. Jing, C. Ze-hua, and He Hai-wu, "Byzantine consensus algorithm based on gossip protocol," *Computer Science*, vol. 45, no. 2, pp. 20–24, 2018.

[34] Y. Yuan and W. Feiyue, "Status and outlook of blockchain technology development," *Journal of Automation*, vol. 42, no. 4, pp. 481–494, 2016.

[35] Z. Long, Z. Xianwei, W. Jianping, D. Yu, and Wu Qiwu, "Routing protocols in tolerant latency and tolerant break networks," *Journal of Software*, vol. 21, no. 10, pp. 2554–2572, 2010.

[36] Z. Wang, X. H. Wang, and J. Q. Sui, "A study on opportunity network simulator ONE and its extensions," *Computer Application Research*, vol. 29, no. 1, pp. 272–277, 2012.

[37] Z.-Y. Yu, *Improved Prophet Routing in Delay-Tolerant Networks*, Nanjing University of Posts and Telecommunications, Nanjing, China, 2015.