Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.049970

REVIEW

Towards Blockchain-Based Secure BGP Routing, Challenges and Future Research Directions

Qiong Yang[1], Li Ma[1,2,*], Shanshan Tu[1], Sami Ullah[3], Muhammad Waqas[4,5] and Hisham Alasmary[6]

[1]Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China

[2]School of Information Science and Technology, North China University of Technology, Beijing, 100144, China

[3]Department of Computer Science, Shaheed Benazir Bhutto University, Sheringal, 18050, Pakistan

[4]School of Computing and Mathematical Science, Faculty of Engineering and Science, University of Greenwich, London, SE10 9LS, UK

[5]School of Engineering, Edith Cowan University, Perth, 6027, Australia

[6]Department of Computer Science, King Khalid University, Abha, 61421, Saudi Arabia

*Corresponding Author: Li Ma. Email: mali@ncut.edu.cn

Received: 23 January 2024 Accepted: 04 March 2024 Published: 15 May 2024

ABSTRACT

Border Gateway Protocol (BGP) is a standard inter-domain routing protocol for the Internet that conveys network layer reachability information and establishes routes to different destinations. The BGP protocol exhibits security design defects, such as an unconditional trust mechanism and the default acceptance of BGP route announcements from peers by BGP neighboring nodes, easily triggering prefix hijacking, path forgery, route leakage, and other BGP security threats. Meanwhile, the traditional BGP security mechanism, relying on a public key infrastructure, faces issues like a single point of failure and a single point of trust. The decentralization, anti-tampering, and traceability advantages of blockchain offer new solution ideas for constructing secure and trusted inter-domain routing mechanisms. In this paper, we summarize the characteristics of BGP protocol in detail, sort out the BGP security threats and their causes. Additionally, we analyze the shortcomings of the traditional BGP security mechanism and comprehensively evaluate existing blockchain-based solutions to address the above problems and validate the reliability and effectiveness of blockchain-based BGP security methods in mitigating BGP security threats. Finally, we discuss the challenges posed by BGP security problems and outline prospects for future research.

KEYWORDS

BGP security; blockchain; prefix hijacking; trust model; secure routing

Nomenclature

BGP	Border Gateway Protocol
ASs	Autonomous Systems
ASN	Autonomous System Number
PKI	Public Key Infrastructure
RPKI	Resource Public Key Infrastructure

NLRI	Network Layer Reachability Information
CIDR	Classless Inter-Domain Routing
CXPST	Coordinated Cross Plane Session Termination
DDoS	Distributed Denial of Service
SIDRW	Secure Inter-Domain Routing Working Group
ROA	Route Origination Authorizations
P2P	Peer-to-Peer
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
API	Application Programming Interface
DINRMS	Decentralized Internet Number Resource Management System
INR	Internet Number Resource
IPRV	Inter-domain Prefix and Route Validation Framework
SBFT	Speculative Byzantine Fault Tolerant
BRVM	Blockchain-based Routing Verification Model
TEE	Trusted Execution Environment
IRPC	Inter-domain Routing Policy Compliance validation

1 Introduction

The inter-domain routing system consists of numerous distributed Autonomous Systems (ASs), each managed independently by its own administrative body and distinguished by a unique Autonomous System Number (ASN), which interconnects using BGP [1]. The inter-domain routing system can be divided into two components: A control plane, responsible for determining packet forwarding destinations, and a data plane, which carries out the actual packet forwarding [2]. Due to the importance of BGP in the Internet, the security of BGP is of great significance for the safe and reliable operation of the Internet [3]. However, the BGP protocol has a security design defect, i.e., an unconditional trust mechanism, which exposes BGP routes to malicious attacks or misconfigurations, triggering BGP security threats such as prefix hijacking, path forgery, and route leakage. These problems lead BGP to hijack traffic, redirection, and network disruptions, affecting Internet connectivity [4].

Traditional BGP security mechanisms are based on the centralized architecture of Public Key Infrastructure (PKI) and Resource Public Key Infrastructure (RPKI) [5], which are prone to a single point of failure and a single point of trust problems [6]. Additionally, they introduce challenges like computational overhead, which can be burdensome for existing routing devices. The complexity of management poses difficulties for network administrators to comprehend, and deployment can be challenging, requiring collaboration among multiple parties. Researchers have recently started experimenting with applying blockchain technology to inter-domain routing systems [7–9]. Blockchain stores data in blocks and forms chains chronologically to ensure that the data are not tampered with and traceable [10]. The peer-to-peer network communication mechanism of blockchain gives blockchain its decentralized nature. Combining cryptography technology and a consensus mechanism in blockchain establishes trust relationships between nodes and ensures data consistency and integrity [11]. The decentralized, tamper-proof, and traceable characteristics of blockchain can solve the single point of failure and single point of trust of centralized trust centers. It establishes reliable trust relationships for inter-domain routing, and nodes can establish a centerless trust between them to form a trusted inter-domain routing system.

Due to the unconditional trust mechanism of BGP, it is impossible to establish a trustworthy relationship between ASs. The traditional BGP security mechanism uses RPKI as the centralized architecture, which is prone to single-point failure and single-point trust problems. The combination of BGP and blockchain solves the single-point failure and single-point trust problems of the traditional centralized architecture by using the blockchain's unique attributes of decentralization, tamper-proofing, and traceability to establish a transferable trust relationship between ASs. However, combining BGP and blockchain is not a complete replacement for RPKI but provides an alternative to enhance BGP security. Although blockchain technology can provide a new solution to the trust problem of inter-domain routing, blockchain-based BGP security research has limitations, such as the compatibility of blockchain and BGP, blockchain security, and data privacy.

This paper aims to provide an up-to-date and comprehensive review of blockchain-based BGP security research to provide a reference for those working on BGP security research. This paper analyzes how blockchain technology can implement alternatives to prevent BGP security threats such as prefix hijacking and route leakage. This paper reviews the progress of blockchain-based BGP security research, discusses the barriers encountered in current research, and provides possible research directions for future research.

Our contributions are summarized as follows:

(1) We sort out BGP security threats and analyze the reasons for their causes;

(2) We analyze the traditional BGP security mechanism and dissect the shortcomings of the existing RPKI-based BGP security mechanism;

(3) We analyze the idea of combining blockchain technology with BGP, focusing on the research progress of blockchain technology in the field of BGP security;

(4) We point out the problems of blockchain technology in BGP security and discuss the challenges of BGP security research and research outlook.

The rest of this paper is organized as follows. In Section 2, we summarize the characteristics of the BGP protocol. In Section 3, we sort out BGP security threats and analyze the reasons for their causes. Section 4 dissects the defects of the traditional BGP security mechanism. We analyze blockchain technology and the idea of combining it with BGP and review the latest progress of blockchain-based BGP security research in Section 5. We explore BGP security research challenges and research outlook in Section 6. Finally, Section 7 concludes the paper.

2 Overview of BGP

BGP is a standard inter-domain routing protocol for the Internet that connects many ASs to transmit Network Layer Reachability Information (NLRI) and to establish routes to different destination nodes or networks. BGP uses TCP as the underlying transport protocol for routing exchange between ASs and establishes BGP sessions over TCP connections to exchange BGP routing information. BGP routing information is exchanged in incremental updates rather than periodic updates to save network resources and bandwidth. The main characteristics of BGP compared to other routing protocols are the uniqueness of its route propagation method and the flexibility of its routing policy [12].

BGP carries two important path information when propagating routes; one is NLRI, and the other is path attribute. The path information indicates the reachable network topology for reaching the destination route to facilitate routing. The NLRI contains the IP address prefix and length to identify the Classless Inter-Domain Routing (CIDR). The path attribute is used to describe the attributes of the arrival CIDR. The routing policy is specified by AS, including the received routing policy, the externally announced routing policy, and the selection of the best routing policy. The commercial relationship between ASs usually influences the formulation of routing policies by AS. An AS has three primary commercial relationships: 1) customer-provider, 2) provider-customer, and 3) peer-to-peer.

BGP is a path vector routing protocol that passes NLRI between individual ASs, indicating how to reach prefixes. Each BGP route contains a list of ASNs that reach the destination network or path of a node, called AS_PATH. The BGP routing system uses this path vector information to establish a loop-free network topology map of the autonomous system. The Gao-Rexford model, jointly proposed by Gao and Rexford, or the GR model [13], is the standard routing policy model widely used today. This model comprehensively takes into account the primary commercial interests of each AS. According to the inbound policy of the GR model, routes from neighboring customer ASs are preferred over routes from neighboring peer ASs and neighboring provider AS, i.e., customer priority (customer>peer>provider). When the priority is the same, the route with the shortest path is selected. According to the outbound policy of the GR model, routes from customer AS can be announced to all neighboring ASs. In contrast, routes from peer AS or provider AS can only be announced to neighboring customer ASs, adhering to the “valley-free principle.”

BGP is a dynamic routing protocol used to exchange routing information between different ASs. Routers that can execute BGP are called BGP speakers [14], and BGP speakers can advertise BGP messages to the outside world. BGP consists of four types of messages, namely, OPEN messages, UPDATE messages, KEEPALIVE messages, and NOTIFICATION messages. BGP peers are formed by establishing a BGP connection between the BGP speakers and exchanging routing messages with each other. The working of BGP consists of the following four phases:

(1) Neighbor discovery

First, BGP speakers need to establish a peer relationship with their neighboring routers to exchange routing information. The BGP speaker sends the OPEN message to establish a BGP connection with the BGP peer after a successful TCP connection.

(2) Exchanging routes

After BGP peers establish a neighbor relationship, they can exchange routing information. BGP peers exchange routing information by sending UPDATE messages. UPDATE messages are the key BGP messages, including NLRIs and path attributes. UPDATE messages can announce reachable and withdrawn routes. In addition, KEEPALIVE messages are sent periodically between BGP peers to test the validity of a BGP connection. When an error is detected, a BGP router sends a NOTIFICATION message to its peer to interrupt the BGP connection. After a period of time, each BGP peer will have routing information for the entire network.

(3) Calculating routes

Each BGP router will execute the corresponding routing algorithm and calculate its routing table according to its configuration.

(4) Maintaining routes

BGP peers send heartbeat packets to each other periodically to sense the network failure; if the heartbeat packet times out, it is considered that the neighbor relationship does not exist. The BGP router will automatically remove the failure path and update the routing table.

3 BGP Security Threat Analysis

The BGP protocol prioritizes operational efficiency, paying minimal attention to trust issues and the security of participating network entities. BGP is designed with the implicit assumption that any BGP router accessing the Internet is trustworthy or that the network operator accessing the Internet is trustworthy. The unconditional trust mechanism of BGP has led to many BGP security threats to inter-domain routing systems. Fig. 1 provides a chronological list of notable BGP security events, each with varying degrees of impact on the stability and availability of the Internet.

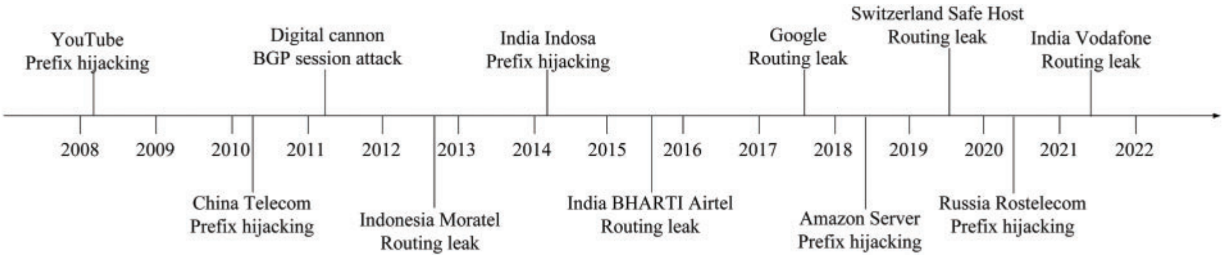

Figure 1: BGP security events

3.1 *Prefix Hijacking*

Prefix hijacking refers to an AS announcing routing information to its neighboring AS that does not belong to its IP prefix address range. Since BGP cannot verify the authenticity of the prefix source routing information, neighboring ASs are likely to accept the wrong route announcement and redirect packets to the prefix-hijacked autonomous system [15]. Prefix hijacking is the most significant BGP security threat, which not only destroys the network accessibility and security of the hijacked network but also may lead to large-scale disruption of the entire Internet. For example, the malicious YouTube routing hijacking incident [16] resulted in up to two hours of global user access. As shown in Fig. 2, node A is the legitimate owner of the prefix P. A normally advertises the route outward, and E maliciously advertises the ownership of the prefix P. Since D cannot verify who the legitimate owner of the prefix P is between A and E, D will choose to go from E to prefix P based on the shortest path. Therefore, E hijacks the traffic from D to A.

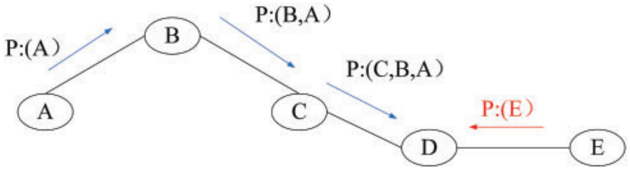

Figure 2: Prefix hijacking in BGP

3.2 Path Forgery

Path forgery means that an AS tampers with the AS_PATH path attribute when announcing routes to its neighboring ASs. Since BGP cannot verify the authenticity of the path attribute, an attacker can tamper with the AS_PATH attribute to influence the routing of other neighboring ASs. Hence, it generates traffic redirection and results in network disruption and traffic eavesdropping. As shown in Fig. 3, node E issues a false route announcement to node D, i.e., only a one-hop path P:(E, A) from E to A. D also receives a route announcement to A issued by C. D cannot judge the authenticity of the two paths from C to A and E to A. D will choose the false route announced by E based on the shortest path, causing network traffic to be unreachable.

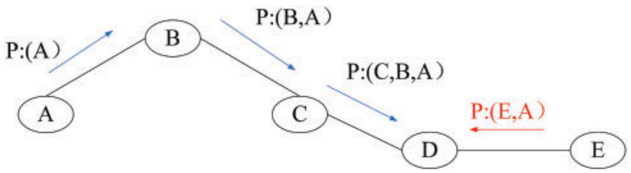

Figure 3: Path forgery in routing

3.3 Route Leakage

Routing leakage has not been clearly defined. RFC 7908 [17] defines routing leakage as the propagation of routes beyond the expected range. In essence, it occurs when an AS violates the receiving routing policy, the externally announced routing policy, and the selection of the best routing policy while announcing routes to neighboring ASs. Route leakage can cause unintended traffic redirection, leading to traffic black holes and traffic eavesdropping. Route leaks can cause serious errors in BGP routing and are a serious BGP security threat that leads to Internet interruption. For example, the Google routing leak [18] in 2017 caused a large number of users in Japan to be disconnected for one hour. Fig. 4a shows the route announcement violation notice obtained by the AS from the provider to another provider and peer. Fig. 4b shows the route announcement violation notice obtained by the AS from the peer to another peer and provider.

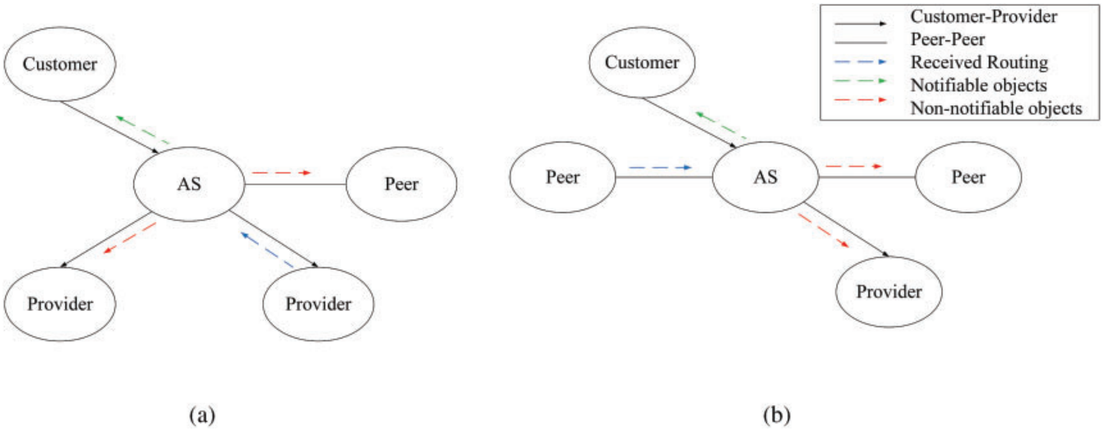

Figure 4: Route leakage from provider and peer. (a) shows the route announcement violation notice obtained by the AS from the provider to another provider and peer. (b) shows the route announcement violation notice obtained by the AS from the peer to another peer and provider

3.4 Route Flap

Route flap [19] is a phenomenon in which BGP repeatedly announce and withdraws route updates. This "unstable" routing phenomenon is suppressed when BGP routes are frequently announced and repeatedly withdrawn. It necessitates finding an alternative path for IP network traffic from the victim's network to the Internet and re-routing. If no alternative BGP route can be found, network connectivity from the victim's network to the Internet becomes unreachable during the route suppression. Mao et al. [20] showed that re-announcing BGP routes immediately after revocation also triggers a routing jitter mechanism that affects the victim's network connectivity and even disrupts the network for up to one hour.

3.5 BGP Session Attack

BGP uses TCP as the underlying transport protocol for exchanging route information between ASs and establishes BGP sessions over TCP connections. Therefore, attacks against TCP also pose risks to BGP security. An attacker can use session hijacking, session reset and other related means to disrupt or interfere with the sessions of two BGP peers [21,22]. The BGP session between two peers should always be connected. If an attacker can reset the BGP session between two peers, it will lead to route revocation, affecting network reachability and even causing the entire Internet to go down. Schuchard et al. [23] proposed the Coordinated Cross Plane Session Termination (CXPST) attack, or "digital cannon", based on the Distributed Denial of Service (DDoS) attack proposed by Zhang et al. [24]. The CXPST attack causes BGP sessions to be repeatedly reset, resulting in a large number of BGP routing update messages to core routers on the Internet. This results in excessive CPU load on the router, severely affecting the routing performance on the Internet.

3.6 Misconfiguration

Misconfiguration refers to an error made by a network operator while configuring BGP routing information rather than an intentional attack on BGP routes. Despite being unintentional, misconfiguration can yield effects and damage similar to a malicious attack, posing challenges in distinguishing between the two. For example, the Google routing leak in 2017, where Google unintentionally leaked routing information obtained from its peers to its providers, resulted in a large number of users in Japan being unable to connect to the network.

Table 1 lists the attack type, launch mechanism, and severity of BGP attacks. In summary, the various BGP security threats in the inter-domain routing system are ultimately due to the security vulnerability of the inter-domain routing system control plane. The security vulnerability of the inter-domain routing system control plane mainly stems from the inherent security flaw of the inter-domain routing system. The flaw includes the inability to establish a trustworthy trust relationship among ASs to verify the authenticity of routing information or not. With the growing number of devices connecting to the Internet, the network topology and cooperative relationships between ASs have become more complex [25]. To deliver inter-domain routing information with guaranteed authenticity and integrity, the inter-domain routing system requires the participants to deliver BGP routing information to establish a transferable trust relationship from the source of the information. With the large number of distributed autonomous networks connected to the Internet, it is increasingly difficult to establish such trust transfer relationships. For this reason, many researchers have conducted studies to address this problem [3,4].

Table 1: Summary of BGP attacks

Attack type	Launch mechanism	Severity
Prefix hijacking	Since BGP cannot verify the authenticity of the prefix source routing information, the AS externally announces illegitimate prefix hijacking traffic	Destroys the accessibility of the hijacked network, leading to network paralysis in severe cases
Path forgery	Since BGP cannot verify the authenticity of the path attribute, the AS tampers with the AS_PATH path attribute when announcing routes externally	Generate traffic redirection, leading to network disruption and traffic eavesdropping
Route leakage	AS violates routing policy when announcing routes externally	Unintended redirection of traffic is also a serious BGP security threat that leads to Internet interruption
Route flap	AS frequently issuance and then withdraws routing update announcements, triggering the routing jitter suppression mechanism	It affects the victim's network connectivity and can also lead to service disruptions
Session attack	An attacker can use session hijacking, session reset, and other related means to disrupt or interfere with the sessions of two BGP peers	This causes routes to be withdrawn, affecting network reachability and even causing network paralysis
Misconfiguration	An error occurs when the network operator configures BGP routing information	It can yield similar effects and damage as a malicious attack

4 Traditional BGP Security Mechanism

Research on inter-domain routing security has been ongoing for more than two decades. Due to the importance of BGP security on the Internet, BGP security research has been a hot spot in academic research. Researchers have conducted studies to enhance BGP security, aiming to address deficiencies in the security design of BGP. These efforts primarily fall into two categories. The first category involves employing security certificates, digital signatures, and encryption technologies to compensate for the absence of route authentication in BGP, thereby enhancing the security mechanism of the BGP protocol. The second category focuses on various BGP route detection studies based on intrusion detection ideas, which can detect abnormal BGP routing events but cannot prevent the occurrence of BGP threat events. As an important Internet infrastructure, BGP protocol should strengthen the prior defense mechanism, improve route authentication, and enhance the security of inter-domain communication. In this paper, we select typical BGP security mechanisms for analysis and start from the contents of S-BGP, S-BGP distributed optimization, and RPKI & ROA & BGPsec.

4.1 S-BGP

Kent et al. [26] proposed S-BGP, the earliest literature on enhancing BGP security [27]. S-BGP uses a centralized hierarchical trust model based on PKI technology to verify routing information using public key certificates and digital signatures to solve the routing authentication problem that exists in BGP. S-BGP draws on the model of assigning IP addresses as well as AS numbers to Internet resources to establish a PKI system that can be parallel to it. S-BGP uses two PKI structures (one for address allocation and the other for assigning AS and router associations), four types of certificates (including root certificates, Internet registry certificates, Internet service provider certificates, and subscriber certificates) for verifying the ownership of IP addresses, AS numbers, and the identity of routers. In addition, S-BGP is designed to use digitally signed address proofs and route proofs to verify the authenticity of source routes and the integrity of path information in route announcements using the above-mentioned public key certificates. S-BGP builds one of the most comprehensive architectures for solving BGP route authentication. Still, S-BGP is not deployed because of its high computational overhead, long path convergence, and the need to involve multiple parties in building PKI.

4.2 S-BGP Distributed Optimization

To address S-BGP problems, Cisco proposed soBGP [28] based on S-BGP research. soBGP achieves routing authentication through three types of certificates: An entity ID certificate that verifies the AS, an authorization certificate that announces the IP address block, and a certificate that reflects the AS topology relationship. soBGP uses a web of trust model to verify the identity of AS through a well-known third-party certification public key authentication by a service provider. The higher-level AS that owns the address block that gives authorization signature to its lower-level AS. Viewing the public key of higher-level, AS can verify whether the AS has the right to advertise the IP address block. The certificate of AS topology relationship contains a list of each AS and its connected peers, from which the topology map of AS is constructed, and the authenticity of the AS_PATH path attribute in the route announcement can be verified. soBGP does not need to build a PKI system, which is relatively simple, but it cannot evaluate the trust degree of each AS in the web of trust model. It is a lightweight BGP security mechanism that sacrifices security.

psBGP [29] established distributed trust management through the evaluation mechanism of AS to achieve route source authentication and path authentication among ASs. psBGP simplifies the method of route source authentication by using a web-of-trust model to verify the ownership of IP prefixes. Each AS has a prefix declaration list, which records the network prefixes of a certain AS and their neighbors. By viewing the prefix declaration list of an AS neighbor, the route source information advertised by that AS can be verified. Moreover, the legitimacy of the network prefixes advertised by that AS can be proved through the neighbor. psBGP does not need to manage a large number of certificates, which reduces the computational overhead and is a lightweight BGP security mechanism. However, the evaluation mechanism of psBGP is challenging to guarantee that the proofs among neighboring ASs are all trustworthy, and collusion may occur among ASs, thereby reducing the security capability of psBGP.

4.3 RPKI & ROA & BGPsec

In view of the security problems associated with BGP, the Internet Engineering Task Force established the Secure Inter-Domain Routing Working Group (SIDRW) to propose solutions to BGP security threats. The SIDRW proposed the first standardized architecture for RPKI [30]. This architecture prevents prefix hijacking by recording the mapping relationship between prefix addresses and the autonomous systems authorized to use their prefix addresses. Route Origination Authorizations (ROA) [31] use distributed storage to bind the prefix address to the AS sequence number of the routing source AS. Each AS is authenticated by ROA information, which can verify whether the source AS has the right to advertise NLRI. To prevent the occurrence of path forgery, BGPsec [32] based on RPKI architecture is proposed. It uses RPKI to issue certificates for AS and prefix addresses, employing signatures to authenticate AS paths, effectively addressing the issue of path forgery. Although RPKI & ROA & BGPsec have played an important role in the field of inter-domain routing security, there are still unresolved security issues with complex management, deployment difficulties, and centralized trust architecture [33–36].

Based on the above analysis, Table 2 lists the trust model, trust mechanism, security authentication, and security problems of the traditional BGP security mechanism.

Table 2: Comparison of traditional BGP security mechanisms

Security mechanism	Trust model	Trust mechanism			Security authentication		Deficiencies
		CA	Digital signature	Encryption	Source	AS Path	
S-BGP [26]	Centralized	√	√	√	√	√	PKI security risks
soBGP [28]	Distributed	√	×	×	√	×	Trust degree
psBGP [29]	Distributed	√	×	×	√	√	Evaluation risks
RPKI & ROA & BGPsec [30–32]	Centralized	√	√	×	√	√	RPKI security risks

Due to the shortcomings of the above traditional BGP security mechanism, there is still a need to explore BGP security research that can be decentralized, easily managed, and deployed to ensure the authenticity and consistency of network resource management and routing information. In recent years, the emergence of blockchain technology has provided new ideas for researchers of inter-domain routing [5,6].

5 Blockchain in the Field of BGP Security

This section presents an overview of blockchain technology in the field of BGP security.

5.1 Integration of Blockchain Technology and BGP

The concept of blockchain first originated from Bitcoin, which was proposed by Satoshi Nakamoto in 2008 [37]. Bitcoin is the first cryptocurrency to emerge in the world with decentralized, open, transparent, and tamper-proof characteristics. The emergence of Bitcoin has attracted widespread attention worldwide, and blockchain as its core technology is highly favored by many researchers and scholars [7–9]. Blockchain technology is a distributed infrastructure and computing paradigm. It uses a chain structure to store data chronologically and validates the data within the system. It uses node consensus algorithms to generate and maintain data, cryptography to ensure data transmission and access security, and smart contracts to write scripting code and automate the operational process [38,39].

Blockchain is a decentralized ledger integrating cryptography technology, peer-to-peer network protocols, consensus mechanisms, and smart contracts. It uses an unforgeable and traceable blockchain-style structure to store data. In a peer-to-peer network environment, information is transmitted point-to-point, and cryptographic techniques and consensus mechanisms are used to ensure that transactions are trusted. Hence, this approach can solve the data trust problem in distributed systems. Blockchain has the characteristics of unforgability, decentralization, transparency, and trustworthiness. Users can verify the data on the chain to prevent data from being tampered with inconsistently. The blockchain system structure can be generally divided into five layers: The data layer, network layer, consensus layer, smart contract layer, and application layer, as shown in Fig. 5.

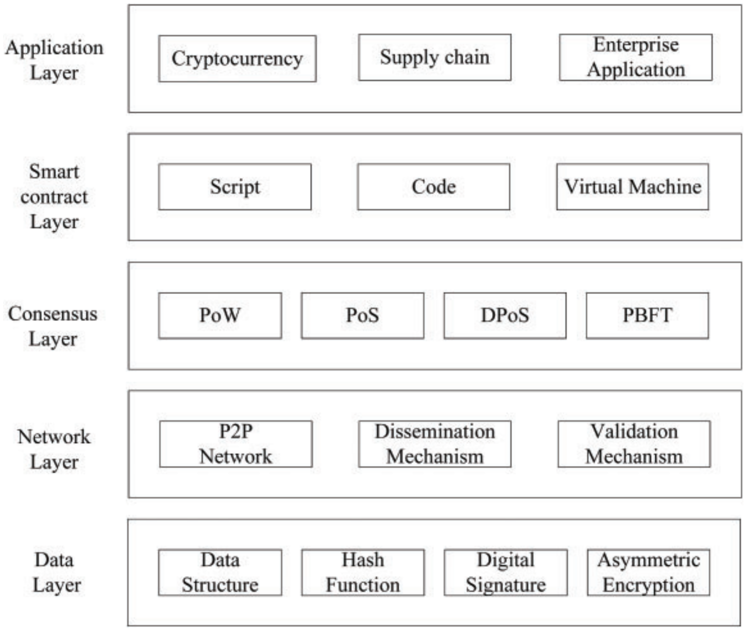

Figure 5: The structure of the blockchain system

(1) Data layer

The data layer is the bottom layer of the blockchain system structure. It mainly contains the data structure of the blockchain, combined with the cryptographic mechanism, to ensure the security and integrity of the data. The data in the blockchain is stored in the block, which in turn consists of two parts: The block head and the block body, as shown in Fig. 6. The storage of data is based on the Merkle tree, which is a binary tree composed of a set of hash values, where the leaf nodes store the hash values of transactions, the intermediate nodes are composed of the hash values calculated by their left and right children, and the root node of the binary tree, called Merkle root. The role of the Merkle tree is to locate transactions and achieve integrity verification of individual transactions quickly. The block header includes the hash value of the previous block, the Merkle root, the hash value of the current block, and other fields, which include a timestamp and random number. The block body is a part of the Merkle tree, excluding the Merkle root. The data in the blockchain is stored in blocks, forming a chain according to the time dimension. Except for the Genesis block, each block contains the previous block's hash value, making the data tamper-proof and traceable.

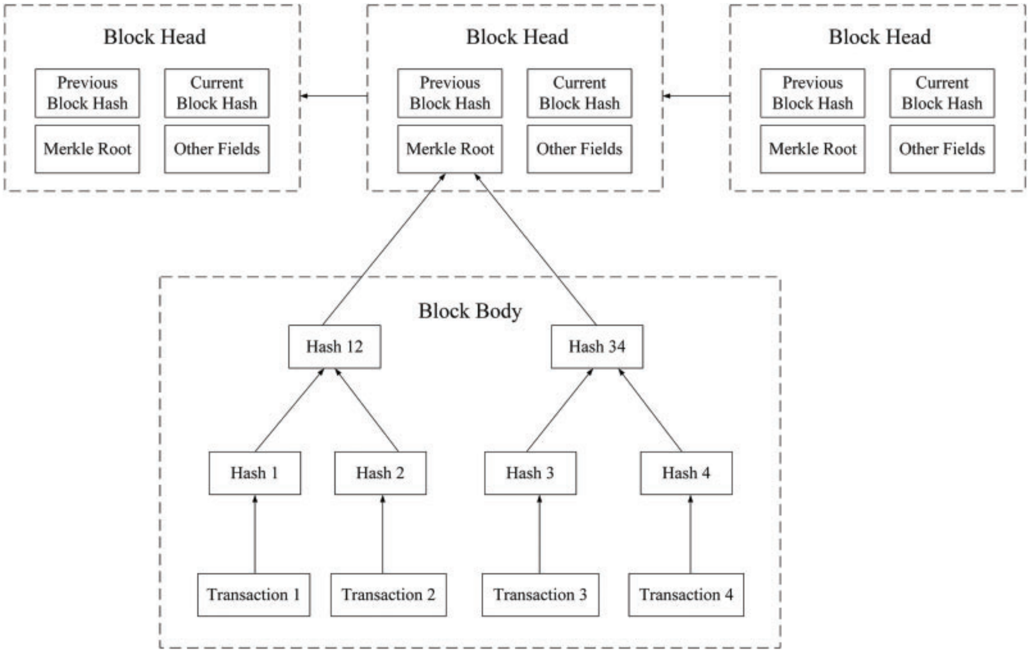

Figure 6: Blockchain data structure

(2) Network layer

The network layer mainly completes the interconnection and data interaction between nodes. The network layer primarily utilizes the Peer-to-Peer (P2P) protocol, facilitating the direct exchange of shared information among nodes. In a P2P network, all nodes possess equal status, and no central control node exists. Each node functions as a service requester and a service provider, establishing a flat topology among nodes. This flat topology is the origin of the decentralized nature of blockchain. Upon joining a P2P network, a single node establishes neighbor relationships by connecting to multiple adjacent nodes. The data, including transactions and blocks generated by the node, is then broadcast to the entire network through these neighboring nodes. Each node stores the received transaction and blocks data locally to build the local blockchain. Each node maintains a copy of the data, and mutual backups among nodes ensure that data destruction on one node does not affect the global picture. This distributed blockchain architecture can effectively avoid the risk of single-point failure of centralized architecture and improve the system's overall efficiency.

(3) Consensus layer

The consensus layer mainly achieves the consistency and integrity of data on the blockchain through consensus mechanisms. The consensus mechanism can establish a trust relationship between non-trusted nodes. Therefore, the data on the blockchain can still reach a final agreement even if there are malicious nodes or node failures. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). PoW first appeared in Bitcoin's transaction system, called "mining". PoW consumes many resources to compete for bookkeeping rights, affecting performance efficiency. PoS can appropriately reduce the resource consumption of competing for accounting rights, yet it is easy to form asset centrality as assets increase. DPoS is similar to the voting election, which does not consume a lot of resources and can shorten the consensus-reaching time but is not easily regulated. PBFT has strong adaptability, low resource consumption, and high efficiency but poor scalability and fault tolerance. The consensus process solves the trust problem between nodes and prevents the single point of trust problem.

(4) Smart contract layer

Smart contracts represent digital promises, employing a computer language to code a program that executes the agreed-upon terms akin to the terms outlined in a legal contract. Smart contracts are deployed on a blockchain virtual machine, ensuring they do not interact directly with the network or other processes to achieve secure isolation. The smart contract automatically runs and validates the protocol program according to predefined trigger conditions and can be executed automatically without human intervention. Once a smart contract is deployed and running, it cannot be modified at will unless the trigger conditions for executing the next smart contract are met. This approach ensures efficient and accurate execution of smart contracts and reduces the risk of human intervention. In the blockchain, smart contracts are executed automatically, and the execution results are stored on the blockchain. Based on the consensus mechanism, nodes across the network can execute smart contracts and agree on the execution results, ensuring that the execution results are not tampered with.

(5) Application layer

The application layer provides users with services for cryptocurrency, supply chain, and other application scenarios. This is accomplished by interacting and exchanging data with smart contracts' user-friendly Application Programming Interface (API).

The fundamental purpose of blockchain is to address data reliability and trust issues in transactions [40]. The unique properties of decentralization, tamper-proof, and traceability of blockchain align with the characteristics of the distributed autonomous system of the inter-domain routing system. This alignment can provide favorable technical support for building trusted inter-domain routing. When each AS executes or keeps local routing policies and business rules, blockchain can become an infrastructure for establishing a common trust relationship among ASs on the Internet. By leveraging this mechanism and engaging in inter-domain multi-party cooperation, it becomes possible to construct an organized and trustworthy inter-domain routing system.

The existing RPKI-based inter-domain routing mechanism uses a centralized certificate management mechanism with a large certificate scale and complex management. Moreover, the existing RPKI inter-domain routing mechanism based on centralized RPKI architecture has a single point of failure and a single point of trust problems. This undermines the reliability of the data source upon which the inter-domain routing algorithm depends. It is possible to build a real storage platform through blockchain technology to store information for security verification of inter-domain routing. The verification process is done jointly by nodes on the blockchain. The current inter-domain routing system lacks a trustworthy incentive mechanism to coordinate the collaboration among organizations and motivate them to strengthen inter-domain trust cooperation. Blockchain technology provides a new solution to the above problem. Table 3 presents the RPKI inter-domain routing mechanism, its defects, the advantages of blockchain technology, and blockchain solution ideas.

5.2 Progress of Blockchain-Based BGP Security Research

Building a decentralized trust model based on the blockchain can eliminate the trust risk of the centralized architecture of an inter-domain routing system. Researchers have recently started adopting blockchain technology to solve the trust problem in inter-domain routing. Hari et al. [41] proposed an Internet Blockchain where Internet resources such as IP network prefixes and ASNs are considered assets in a blockchain. Operations such as asset allocation, distribution, and BGP routing announcements are considered transactional activities in this framework. Blockchain technology is used for the trusted management of digital number resources throughout their lifecycle on the Internet.

Table 3: Summary of the integration of blockchain technology and BGP

RPKI mechanism	Defects of RPKI mechanism	Advantages of blockchain	Blockchain solution
Routing authentication based on RPKI	Management complexity	Tamper-proof, distributed	Build an RPKI authentication
	Deployment difficulties	Incentives	Reduce deployment difficulty
	Centralized trust architecture	Distributed repository	Store routing information

Blockchain is mainly used as a repository in the inter-domain routing domain. It is leveraging blockchain's decentralized and non-tampering nature to establish a distributed, secure and trusted repository for inter-domain routing. Existing research is divided into three main categories. Firstly, it involves utilizing blockchain to create a decentralized authentication architecture with functionality similar to RPKI. This includes establishing a straightforward and efficient trust model and management system for resource management (e.g., [42,43,44–47]), encompassing tasks such as IP address and ASN management, as an alternative to RPKI. Secondly, route authentication (e.g., [41,48–57]) is achieved via blockchain, encompassing both source route authentication and path authentication. This involves verifying the ownership of source routes and confirming the consistency of AS_PATH attribute information in BGP route announcements with the actual propagation path. This is accomplished by referencing the information stored on the blockchain, thereby enhancing the capabilities of RPKI. Thirdly, the blockchain is the repository for routing policies (e.g., [58–61]). These policies are uploaded onto the distributed ledger of the blockchain to prevent routing leaks, ensuring the verification of routing policy information.

5.2.1 Resource Management

Blockchain is applied to Internet resource management for IP address management or ASN management to establish a more effective trust model than RPKI and a management system. Xing et al. [42] proposed BGPcoin, an Ethernet blockchain-based solution for Internet resources. BGPcoin uses smart contracts on the Ethernet blockchain to achieve authorization of IP addresses and AS serial numbers and to resist prefix hijacking. There are two main components in BGPcoin. One is the smart contract, which is used as an interface for resource management. The other is a client that interacts with smart contracts and provides users with search resources. In this component, each AS maintains its Ethernet smart contract client. Xing et al. [43] extended BGPcoin based on the literature [42] by adding ROA authentication to replicate the network resource registration, allocation, and distribution process. BGPcoin obtains the legal authorization of the IP network prefix and the ASN by querying the Ethernet client of the AS. BGPcoin is based on the Ethereum platform and employs the PoW consensus algorithm. However, this approach is susceptible to data forking, resulting in inconsistent routing authentication data and introducing new security risks.

Paillisse et al. [44] proposed IPchain, which uses blockchain to ensure the authenticity and traceability of the process of IP address distribution down the hierarchy. IPchain stores all the information of IP addresses in the blockchain to reduce the security risk of RPKI. IPchain uses asset-based equity to prove the consensus mechanism of PoS. Although PoS has the potential to decrease storage overhead while maintaining security, its consensus mechanism may result in entities possessing a significant number of network resources gaining greater control. This is contrary to the objective of leveraging blockchain to achieve the decentralization of network resources.

Angieri et al. [45] proposed InBlock, a distributed autonomous organization that uses smart contracts from Ether to enable IP address management. Any entity that pays virtual currency to InBlock can request an address assignment. InBlock provides a distributed, automatically executable, publicly transparent, anonymous IP assignment mechanism. InBlock uses distributed consensus for trust management and acts as an authoritative database to guarantee the security of the routing system. Considering that most IPv4 addresses are already allocated, this work only conducts distributed experiments by selecting some addresses in the IPv6 address space.

The literature [46] introduces distributed autonomous organizations for Internet resource management and proposes a trust model to perform ROA functions instead of the hierarchical model of RPKI. The method requires consensus among parties before modifying the existing prefix address assignment information. Moreover, IP addresses are managed through smart contracts without human intervention. This method provides a distributed and publicly accessible resource allocation mechanism for the Internet. The solution can be extended to AS numbers and IPv4 address space and can be applied in IPv6 address space, but it can only manage a scattered subset of address space.

Li et al. [47] proposed a blockchain-based Decentralized Internet Number Resource Management System (DINRMS). DINRMS is a 2-tier Internet Number Resource (INR) management system consisting of an autonomy layer and an arbitration layer, and it uses smart contracts to execute the management logic. ASs in the lower autonomy layer manage the ownership and mapping information of their INRs in groups, and each group elects representatives to participate in the upper arbitration layer. The subgroup representatives record the INR information of their group to the arbitration layer and push the INR information of other subgroups to their group. The arbitration layer stores global INR ownership and mapping information to avoid INR usage conflicts. DINRMS adopts the group hierarchy mechanism to quickly verify the legitimacy of the mapping from the prefix to the origin AS in the update route and defends against prefix hijacking.

Table 4 lists the Internet resource management (IP address management, ASN management) and the BGP security threats (prefix hijacking, path forgery, route leakage, etc.) that can be addressed by blockchain-based BGP security research.

Table 4: Comparison of blockchain-based resource management

Security research	Resource management		Resolved BGP security threats					
	IP	ASN	Prefix hijacking	Path forgery	Routing leak	Routing jitter	Session attack	Miscon figuration
BGPcoin [42,43]	√	√	√	×	×	×	×	×
IPchain [44]	√	×	√	×	×	×	×	×

(Continued)

Table 4 (continued)

Security research	Resource management		Resolved BGP security threats					
	IP	ASN	Prefix hijacking	Path forgery	Routing leak	Routing jitter	Session attack	Misconfiguration
InBlock [45]	√	×	√	×	×	×	×	×
Literature [46]	√	√	√	×	×	×	×	×
DINRMS [47]	√	√	√	×	×	×	×	×

5.2.2 Routing Authentication

Blockchain is applied to BGP route authentication to complete route source authentication or path authentication and enhance the functionality of RPKI. Internet Blockchain [41] is the first to implement blockchain-based BGP route source authentication and path verification. In the Internet Blockchain, the transaction records of Internet resources are stored in the blockchain. The peer entities can verify whether the network resources are valid by querying the transaction records on the blockchain, which can realize route source authentication. In Internet Blockchain, the BGP route announcement transaction takes the upstream AS path as input and the downstream AS that continues to announce the BGP update message as output. The downstream AS adds its preceding ASN to the AS_PATH list when it advertises the BGP update message to achieve path verifiability. Internet Blockchain provides a distributed and tamper-proof framework for BGP route authentication, which belongs to the design phase and has not been implemented.

SBTM [48] constructs a blockchain-based inter-domain routing security trust management system for identity management, route source authentication, etc. SBTM combines blockchain and PKI systems to manage the entity identity and IP network prefix ownership of inter-domain routing. SBTM can eliminate the central single point of failure through a distributed PKI system. However, the SBTM consensus algorithm uses PoW, which is computationally expensive and prone to data forking, leading to data inconsistency and threatening BGP security.

The literature [49] proposes uploading IP prefix addresses to the blockchain. If the IP prefix matches the ROA entry, the AS border router will download the current IP prefix from the blockchain and inform the neighboring nodes about it. This method manages AS router configuration through smart contracts, allowing prefixes to be verified before routers are deployed. This method prevents prefix hijacking but does not include transactions that register AS numbers or revoke allocated resources.

Sfyrakis et al. [50] implemented a prototype system for BGP routing authentication mentioned in Internet Blockchain by Hari et al. [41]. This prototype system stores and verifies transactions related to IP network prefixes and BGP paths. Blockchain-based authentication is employed for routing sources involving operations related to assignment and revocation within IP network prefixes. Additionally, path verification is executed for BGP paths, encompassing operations related to notification and withdrawal. The system standardizes Internet resources such as IP and BGP route announcements as blockchain transactions and uses blockchain to verify BGP route announcements' prefixes and path legitimacy. The prototype system does not change BGP; the blockchain verifies BGP route announcements. Each BGP update is treated as a blockchain transaction, which will cause storage and performance issues.

Saad et al. [51] proposed RouteChain, a two-layer blockchain model, to prevent BGP hijacking and maintain a globally consistent view of routing paths. RouteChain treats BGP route announcements as blockchain transactions and uses the Clique consensus mechanism to reach consensus among ASs. All ASs are divided into subgroups according to the geographical proximity between ASs, and each subgroup shares the ledger. Each AS within the subgroup tracks the routing paths of ASs within the subgroup through the subgroup ledger. By assigning ASs to each subgroup leader, ASs can reach a consensus among themselves quickly. The blockchain structure with two layers can improve performance and reduce latency, but the geographic proximity between ASs cannot map the realistic, logical adjacency situation between domains. Some ASs may be reluctant to accept group leader control due to conflicts of interests or policies.

Chen et al. [52] proposed ISRchain, an inter-domain secure routing authentication framework. ISRchain maintains a consistent view of existing AS and IP network prefix owners and uses smart contracts to verify source routes, BGP routing paths, and routing policy information. ISRchain prevents prefix hijacking, path forgery, and route leakage. This ISRchain does not change the original inter-domain routing architecture and achieves efficient and lightweight routing authentication. However, using the Raft consensus algorithm leads to poor scalability, and the process of electing leaders in consensus is fixed and easily predicted, triggering DoS attacks. In addition, ISRchain requires uploading routing policies and does not consider the confidentiality of routing policies.

A new blockchain-based BGP security infrastructure, ROAchain is proposed in the literature [53]. Each AS maintains a consistent and non-tamperable ROA repository to verify the authenticity and legitimacy of route sources and resist BGP prefix hijacking. All ROA registration, update, and revocation operations are recorded in the ROA repository. Moreover, each AS synchronizes the ROA repository through ROAchain for BGP route origin verification. The literature [54] proposes a novel consensus algorithm based on the literature [53], in which trust values, collective signatures, sharding, and penalty mechanisms are introduced to optimize the consensus algorithm without changing the existing BGP protocol. The algorithm has better scalability and performance than the traditional algorithm, but the sharding mechanism increases complexity.

Podili et al. [55] proposed the Inter-domain Prefix and Route Validation Framework (IPRV) for verifying the ownership of network prefixes exchanged between domains on the Internet and the integrity of routing messages. IPRV can provide prefix and path verifications to achieve cross-domain BGP secure routing. IPRV consists of two main components: A distributed ledger based on a directed acyclic graph and a route validation node. The distributed ledger of the directed acyclic graph records prefix management transactions and BGP routing-related transactions in BGP route announcements. Moreover, the route validation node maintains the distributed ledger of the directed acyclic graph and provides network prefix and route validation services. The distributed ledger of the directed acyclic graph uses the consensus mechanism of authentication proof, which can improve the throughput of the distributed network. However, it increases the complexity of the network structure of the directed acyclic graph as the transaction volume increases.

Lu et al. [56] proposed DRRS-BC, a blockchain-based routing registration framework. DRRS-BC establishes a global ledger of IP address prefixes and ASNs between multiple organizations and ASs to verify BGP source route authentication, which can resist prefix hijacking attacks. DRRS-BC is a decentralized database of routing information built on blockchain, which is jointly established by organizations involved in IP address prefix and ASN allocation and authorization. It records network resource transactions between organizations and consists of four parts: Client, endorsement node, block generation node, and ledger storage node. It uses a Speculative Byzantine Fault Tolerant (SBFT) consensus mechanism to maintain the ledger of network resource transactions. DRRS-BC introduces blockchain to provide tamper-proof and traceable proof of IP address prefix ownership and ASNs, solving the security problems of traditional BGP centralized authentication.

Budi Sentana et al. [57] proposed BlockJack, a system based on consortium blockchain that verifies IP address prefixes and AS sources and can prevent BGP prefix hijacking. BlockJack has three modules: Blockchain, analyzer, and the scheduler. Among them, the analyzer module provides an interface for communication between the blockchain module and the scheduler module, and the scheduler module monitors the BGP routing table. The scheduler module issues filtering commands when the BGP routing table is updated. BlockJack stores ROA information in the consortium blockchain, and the system includes two main functions: Authorization and verification of prefixes. It can handle dynamic multiple attacks arising from changes in BGP attribute values that cause dynamic changes in the best valid routes in the BGP routing table.

Table 5 shows the route authentication (source authentication, path authentication) and the BGP security threats (prefix hijacking, path forgery, route leakage, etc.) that can be solved by the blockchain-based BGP security research completed.

Table 5: Comparison of blockchain-based routing authentication

Security research	Routing authentication		Resolved BGP security threats					
	Source	AS Path	Prefix hijacking	Path forgery	Routing leak	Routing jitter	Session attack	Miscon figuration
Internet Blockchain [41]	√	√	√	√	×	×	×	×
SBTM [48]	√	×	√	×	×	×	×	×
Literature [49]	√	×	√	×	×	×	×	×
Literature [50]	√	√	√	√	×	×	×	×
RouteChain [51]	√	√	√	√	×	×	×	×
ISRchain [52]	√	√	√	√	√	×	×	×
ROAchain [53,54]	√	×	√	×	×	×	×	×
IPRV [55]	√	√	√	√	×	×	×	×
DRRS-BC [56]	√	×	√	×	×	×	×	×
BlockJack [57]	√	×	√	×	×	×	×	×

5.2.3 Routing Policy

Liu et al. [58] proposed the Blockchain-based Routing Verification Model (BRVM) to defend against violation of shortest AS path policy attacks. BRVM is a blockchain-based routing verification model that allows all routing nodes to participate in a multi-party verification system by introducing routing proofs to prevent collusive attacks by multiple routing nodes. BRVM uses Byzantine fault-tolerant delegated equity to prove the BFT-DPOS consensus mechanism with 33% fault tolerance. BRVM can verify whether AS nodes select the local best route from upstream neighboring nodes according to the shortest path policy. Moreover, it can resist collusion attacks by multiple routing nodes by using the technical features of blockchain. However, BRVM only verifies whether the AS violates the shortest path and cannot verify other routing policies other than the shortest path policy.

Galmes et al. [59] proposed a solution based on blockchain to prevent route leakage. The method uses formal language to express the routing policy and stores the routing policy in a blockchain-distributed ledger. It also uses the blockchain architecture to ensure secure communication of the routing policy. The method converts the formal language for expressing routing policies into standard BGP routing filters, and the participant AS executes routing policies to prevent route leakage by downloading and installing the standard BGP routing filters. The method uses a formal language and automatically configures BGP routing filters to prevent misconfiguration. It uses the distributed ledger function of blockchain to ensure encryption security. However, this method requires uploading the routing policy to the blockchain and does not consider the confidentiality of the routing policy.

Yue et al. [60] proposed RLPchain, a privacy-preserving routing leakage protection mechanism based on blockchain and Trusted Execution Environment (TEE). Each AS maintains a globally consistent confidential and tamper-proof inter-domain routing policy repository to detect and prevent routing leaks. The core components of RLPchain are TEE and RLPchain nodes on the blockchain, which are responsible for inter-domain routing policy registration, update, and revocation operations. RLPchain nodes use the PBFT consensus mechanism to maintain the routing policy repository jointly. The RLPchain nodes determine whether a route is leaked by the global policy view they have. RLPchain makes a small change to the BGP system, reducing the deployment complexity and ensuring the security of BGP routing policies but sacrificing some performance. The PBFT consensus mechanism is less fault-tolerant and requires that the number of failed nodes cannot exceed one-third of the total number of nodes.

Chen et al. [61] proposed a blockchain-based Inter-domain Routing Policy Compliance validation (IRPC) scheme to defend against route leakage. IRPC contains two transaction types: Policy expectation and route proof. The AS publishes policy expectations based on requirements, and if it needs to specify an AS to validate the policy expectations, it uses the public key encryption policy expectations of the specified AS. IRPC introduces route proofs, generates route proofs for each update route, and publishes them on the chain to ensure the authentic propagation of routes. Participating ASs synchronize policy expectations and route proofs, configure local BGP routers, and perform routing policy compliance verification on received update routes. The ASs participating in IRPC form a trust overlay network to share routing information and jointly verify the compliance of routing policies, which can realize flexible configuration of routing policies and privacy protection.

Table 6 lists the routing policy (method, privacy) and the BGP security threats (prefix hijacking, path forgery, route leakage, etc.) addressed by the blockchain-based BGP security studies regarding routing policies.

Table 6: Comparison of blockchain-based routing policy

Security research	Routing policy		Resolved BGP security threats					
	Method	Privacy	Prefix hijacking	Path forgery	Routing leak	Routing jitter	Session attack	Miscon figuration
BRVM [58]	Verify the shortest path	×	×	×	√	×	×	×

(Continued)

Table 6 (continued)

Security research	Routing policy		Resolved BGP security threats					
	Method	Privacy	Prefix hijacking	Path forgery	Routing leak	Routing jitter	Session attack	Misconfiguration
Literature [59]	Auto configuration	×	×	×	√	×	×	√
RLPchain [60]	TEE encryption	√	×	×	√	×	×	×
IRPC [61]	Encryption	√	×	×	√	×	×	×

Synthesizing the above analysis, Table 7 lists the summary of blockchain-based BGP security research regarding security issues and security mechanism analysis.

Table 7: Summary of blockchain-based BGP security research

Security research	Security issue	Security mechanism analysis
Internet Blockchain [41]	Routing authentication	Proposes a route authentication framework that uses blockchain to store IP address ownership, source route authorization, and AS path announcement transactions to prevent false BGP announcements
BGPcoin [42,43]	Resource management	Utilizes a set of smart contracts to perform and supervise network resource allocation, verify BGP source routes, and prevent prefix hijacking
IPchain [44]	Resource management	Using blockchain to store IP address allocation and authorization processes, providing a flexible trust model against prefix hijacking
InBlock [45]	Resource management	Utilizes smart contracts to perform IPv6 address management, providing an open and transparent IP allocation mechanism to resist prefix hijacking
Literature [46]	Resource management	Proposes an alternative distributed resource allocation mechanism to RPKI, which utilizes smart contracts to perform IP address management and a blockchain to store address allocation and ROA information

(Continued)

Table 7 (continued)

Security research	Security issue	Security mechanism analysis
DINRMS [47]	Resource management	Adoption of 2-layer DINRMS with autonomy and arbitration layers, using smart contracts to verify the legitimacy of the prefix-to-origin AS mapping in the update route to defend against prefix hijacking
SBTM [48]	Source routing authentication	Proposes an alternative trust management framework that utilizes blockchain to store security information for routing and checks the security information to verify the legitimacy of messages and their publishers
Literature [49]	Source routing authentication	Download the router's IP prefix list, use smart contracts to verify the prefixes assigned to the router, and modify the local BGP configuration to prevent prefix hijacking
Literature [50]	Routing authentication	Utilizes blockchain to store and validate transactions related to IP prefix assignment and BGP paths to that prefix, enabling routing source authentication and path verification
RouteChain [51]	Routing authentication	Adopting a global chain and subgroup chain to form a bi-hierarchical blockchain system, and ASs in subgroups share a consistent view of the path to resisting BGP hijacking
ISRchain [52]	Routing authentication routing leak	Stores Internet resource allocation, AS neighbor updates, and routing policies and uses smart contracts to verify source routes, AS paths, and routing policies to prevent prefix hijacking, path forgery, and route leakage
ROAchain [53,54]	Source routing authentication	BGP routers synchronize ROA repositories from ROAchain to verify the legitimacy of BGP route sources and prevent prefix hijacking

(Continued)

Table 7 (continued)

Security research	Security issue	Security mechanism analysis
IPRV [55]	Routing authentication	Uses blockchain to record multi-signature prefix allocation and BGP route announcement transactions, verifying the ownership of network prefixes and the integrity of routing messages to prevent BGP hijacking attacks
DRRS-BC [56]	Source routing authentication	Proposes a route registration system that uses blockchain to record IP address prefix and ASN allocation and authorization transactions, verify BGP source routes, and defend against prefix hijacking
BlockJack [57]	Source routing authentication	Store IP prefixes as well as their origins, use smart contracts to check if new prefixes are stored in the blockchain, verify IP prefix addresses and AS origins, and prevent prefix hijacking
BRVM [58]	Routing leak	Propose a route verification model to build a route-proof chain with the help of blockchain to verify whether the routing policy complies with the shortest AS path policy and prevent routing nodes from collusion attacks
Literature [59]	Routing leak	Utilizes blockchain to store routing policies described in a formal language and converts the formal language to standard BGP route filtering via a compiler, preventing misconfiguration and route leakage
RLPchain [60]	Routing leak	Blockchain and TEE-based route leakage defense mechanism RLPchain, RLPchain nodes maintain a consistent and encrypted routing policy repository to prevent route leakage while protecting routing policy privacy
IRPC [61]	Routing leak	Propose a routing policies validation method, encrypt the publication policy expectation to prevent route leakage and privacy protection, and introduce route proofs to ensure authentic route propagation

6 Problem Challenges and Research Outlook

The research on blockchain-based BGP security is still in the preliminary exploration stage, and there are still many challenges in the security of BGP, as discussed below:

(1) Compatibility issues

In the existing blockchain-based BGP security research, the role of blockchain is mainly to act as a distributed repository to record BGP routing update notices. Combining BGP and blockchain must solve the compatibility problem of BGP protocol and blockchain. Blockchain publishes blocks periodically, while BGP routing update information needs to be updated in real time. Putting BGP routing update notices on the blockchain, the routing update notices stored on the blockchain are challenging to synchronize with BGP update messages, and there are compatibility problems. Blockchain-based BGP security research should be compatible with the existing routing system without changing the existing BGP protocol. Keeping the BGP update announcements and the blockchain records synchronized without changing the BGP protocol is challenging for blockchain-based BGP security research.

(2) Blockchain security issues

The traditional BGP security mechanism, which uses a centralized architecture based on PKI or RPKI system, is prone to a single point of failure and a single point of trust problems. The unique attributes of blockchain, such as decentralization and tamper-proof, provide a basis for inter-domain routing to establish trust relationships. The trust relationships can eliminate the trust risk of centralized architecture for inter-domain routing. However, introducing blockchain brings a new security risk, namely the security of the blockchain itself. Existing research on blockchain-based BGP security uses different consensus mechanisms to enhance the trust and reliability of inter-domain routing systems. However, these consensus mechanisms can only tolerate some malicious nodes, and attackers will launch malicious attacks on the consensus to control the resources. For example, there was a 51% attack against PoW [62] and a sybil attack against PBFT [63]. Therefore, the security issue of blockchain is also a challenge for the subsequent research of blockchain-based BGP security.

(3) Data privacy issues

The existing blockchain-based BGP security research puts Internet resource management information, routing authentication information, and routing policy information on the blockchain, which faces data privacy issues. The tamper-proof and open and transparent features of blockchain make the data stored publicly visible to the blockchain users. The information related to the BGP protocol, especially the routing policy information, needs to be well protected from data leakage. Therefore, the research of BGP security based on a blockchain needs to consider the data privacy issue, especially how to protect the privacy of routing policies. Nevertheless, it will be a great challenge for the research of BGP security based on blockchain.

(4) Blockchain interoperability issues

Blockchain interoperability reflects the interoperability between blockchains, i.e., the ability of one blockchain and other blockchains to enable the free exchange of data. Existing blockchain-based BGP security research utilizes blockchains to store and verify routing-related information. Blockchains are not independent; a blockchain network needs to transact with other blockchain networks and obtain relevant information. Different blockchains are difficult to collaborate with due to different consensus mechanisms, programming voices, and solutions, and there is a blockchain interoperability problem. How can we design concise, safe and reliable cross-chain protocols to enhance the interoperability between blockchains, which poses a new challenge for the subsequent research on blockchain-based BGP security.

Given the important position of BGP on the Internet, coupled with the fact that blockchain-based BGP security research has just started. Hence, the future security research of BGP is still a hot spot for Internet security research.

(1) Routing Security

Existing research on blockchain-based BGP security focuses on the trust problem in the control plane of inter-domain routing systems. Existing studies implicitly assume that attackers will not infringe on routers. They assume the inter-domain routing control plane provides a completely secure routing service. It tends to solve the problems of prefix hijacking and path forgery of inter-domain routing through the control plane secure routing service. Ignoring the routing service security issue, once the routing service is attacked, the existing security mechanisms fail due to being bypassed. They cannot guarantee the secure operation of the routing protocol. Although blockchain technology can provide technical support for building a trusted inter-domain routing system, routing as a network infrastructure, the security of routing itself is a prerequisite and more important. However, to ensure routing security, research scholars of network security, network equipment suppliers, and network operations managers need to work together, and routing security will become the key to the next-generation trusted Internet. Therefore, the routing security research should be increased to guarantee routing security before accessing the blockchain.

(2) Routing Leak

Routing leaks can create serious BGP security incidents and cause even more damage. Routing policies are complex and variable and usually not open to the public. A malicious attack or misconfiguration can cause a route leakage. Misconfigurations can produce the same effects and hazards as malicious attacks, and inter-domain routing systems cannot distinguish between misconfigurations and malicious attacks. In recent years, researchers have explored the use of blockchain technology to solve the routing leakage problem, but there are routing policy privacy issues. The development direction of future research will be how to protect the privacy of routing policies while ensuring that BGP routing policies are not violated. Therefore, it is necessary to study routing leakage in-depth and reduce the occurrence of routing leakage in the future.

(3) Improving the Scalability of Blockchain

Combining blockchain and BGP requires the blockchain to synchronize with the BGP update message. This puts higher requirements on the scalability of the blockchain. Throughput is one of the main indicators of blockchain scalability. A solution combining blockchain and BGP should improve the throughput level to respond quickly to BGP update routing messages and prevent BGP hijacking. Latency is an important parameter affecting blockchain scalability; subsequent research should focus on latency. The delay should be lower than the convergence time of the average route to prevent the error messages from propagating throughout the network, causing ASs to obtain different routing information and influencing routing decisions to cause routing problems. Therefore, future research should still enhance the scalability of blockchain to provide a secure foundation for inter-domain routing.

(4) Introduction of Artificial Intelligence Technology

BGP hijacking and route leakage are important security threats to BGP. Artificial intelligence has powerful algorithms and models that can handle massive amounts of data and analyze data correlations and trends, which helps provide accurate decisions and predictions. In the future, we can consider using AI technology to automate the detection of BGP hijacking and route leakage attacks, tracking and tracing BGP attack events, automatically generating secure routing policies, and drawing a panoramic view of BGP security based on the combination of blockchain and BGP.

7 Conclusions

BGP holds a crucial role as a standard inter-domain routing protocol in the Internet, and its security profoundly impacts the safe and reliable operation of the Internet. The inherent security flaws of BGP have led to frequent BGP security incidents and attracted a considerable number of researchers to delve into BGP security research. Although traditional security mechanisms enhanced the security of BGP protocol, they pose challenges in complicated management, difficult deployment, and centralized trust architecture. While integrating blockchain and BGP and leveraging the distributed architecture of blockchain, cryptographic technology, and consensus mechanisms. Hence, it establishes a reliable trust relationship for BGP and broadens the solutions for BGP security research. However, the security research of BGP based on blockchain is still in the preliminary stage, and BGP's security problem needs to be solved. This paper has summarized the characteristics of BGP protocol and sorted out BGP security threats and their causes. It also analyzed the shortcomings of conventional BGP security mechanisms and assessed the current state of blockchain-based BGP security research. Additionally, it has delved into the issues and challenges encountered in BGP security research, along with future research directions. Therefore, this paper aims to serve as a valuable resource for individuals involved in BGP security research.

Acknowledgement: The authors would like to express their gratitude for the valuable feedback and suggestions provided by all the anonymous reviewers and the editorial team.

Funding Statement: This research was funded by the National Natural Science Foundation of China, Grant Numbers (62272007, 62001007) and the Natural Science Foundation of Beijing, Grant Numbers (4234083, 4212018). The authors also acknowledge the support from King Khalid University for funding this research through the Large Group Project under Grant Number RGP.2/373/45.

Author Contributions: Conceptualization: Qiong Yang; validation: Sami Ullah, Muhammad Waqas; formal analysis: Shanshan Tu, Hisham Alasmary; writing-original draft: Qiong Yang; writing-review & editing: Qiong Yang, Sami Ullah, Muhammad Waqas; supervision: Li Ma.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Rekhter, T. Li, and S. Hares, “A border gateway protocol 4 (BGP-4),” *RFC 4271*, 2006. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc4271/

[2] T. Wirtgen and O. Bonaventure, “A first step towards checking BGP routes in the data plane,” in *Proc. 2022 ACM SIGCOMM, 2022 Work. Future. Internet Rout. Address.*, Amsterdam, The Netherlands, 2022, pp. 50–57.

[3] L. Mastilak, P. Helebrandt, M. Galinski, and I. Kotuliak, “Secure inter-domain routing based on blockchain: A comprehensive survey,” *Sens.*, vol. 22, no. 4, pp. 1437–1462, 2022. doi: 10.3390/s22041437.

[4] D. Chen, H. Qiu, J. H. Zhu, and Q. X. Wang, “Research on blockchain-based interdomain security solutions,” *J. Softw.*, vol. 31, no. 1, pp. 208–227, 2020.

[5] H. Zou, D. Ma, Q. Shao, and W. Mao, “A survey of the resource public key infrastructure,” *Chin. J. Comput.*, vol. 45, no. 5, pp. 1100–1132, 2022.

[6] K. Xu, S. T. Ling, Q. Li, and B. Wu, “Research progress of network security architecture and key technologies based on blockchain,” *Chin. J. Comput.*, vol. 44, no. 1, pp. 55–83, 2021.

[7] S. Tu, H. H. Yu, A. Badshah, M. Waqas, Z. Halim and I. Ahmad, “Secure Internet of Vehicles (IoV) with decentralized consensus blockchain mechanism,” *IEEE Trans. Veh. Tech.*, vol. 72, no. 9, pp. 11227–11236, 2023. doi: 10.1109/TVT.2023.3268135.

[8] S. Tu, A. Badshah, H. Alasmary, and M. Waqas, “EAKE-WC: Efficient and anonymous authenticated key exchange scheme for wearable computing,” *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 4752–4763, 2024. doi: 10.1109/TMC.2023.3297854.

[9] S. Tu, M. Waqas, A. Badshah, M. X. Yin, and G. Abbas, “Network intrusion detection system (NIDS) based on Pseudo-Siamese stacked autoencoders in fog computing,” *IEEE Trans. Serv. Comput.*, vol. 16, no. 6, pp. 4317–4327, 2023. doi: 10.1109/TSC.2023.3319953.

[10] N. Zahed Benisi, M. Aminian, and B. Javadi, “Blockchain-based decentralized storage networks: A survey,” *J. Netw. Comput. Appl.*, vol. 162, no. 4, pp. 102656–102665, 2020. doi: 10.1016/j.jnca.2020.102656.

[11] M. Graf, D. Rausch, V. Ronge, C. Egger, R. Küsters and D. Schröder, “A security framework for distributed ledgers,” in *Proc. ACM Conf. Comput. Commun. Secur.*, Republic of Korea, 2021, pp. 1043–1064.

[12] S. Li, J. W. Zhuge, and X. Li, “Study on BGP security,” *J. Softw.*, vol. 24, no. 1, pp. 121–138, 2013. doi: 10.3724/SP.J.1001.2013.04346.

[13] L. Gao and J. Rexford, “Stable internet routing without global coordination,” *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 681–692, 2001. doi: 10.1109/90.974523.

[14] M. Kowalski and W. Mazurczyk, “Toward the mutual routing security in wide area networks: A scoping review of current threats and countermeasures,” *Comput. Netw.*, vol. 230, no. 1, pp. 1–20, 2023. doi: 10.1016/j.comnet.2023.109778.

[15] S. Cho, R. Fontugne, K. Cho, A. Dainotti, and P. Gill, “BGP hijacking classification,” in *Proc. 3rd Netw. Traffic Meas. Anal. Conf*, Paris, France, 2019, pp. 25–32.

[16] RIPE NCC, “YouTube Hijacking: A RIPE NCC RIS case study,” 2008. Accessed: Dec. 15, 2023. [Online]. Available: https://www.ripe.net/publications/news/youtube-hijacking-a-ripe-ncc-ris-case-study/

[17] K. Sriram, D. Montgomery, and D. McPherson, “Problem definition and classification of BGP route leaks,” *RFC 7908*, 2016. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc7908/

[18] BGPmon Blog, “BGP leak causing Internet outages in Japan and beyond,” 2017. Accessed: Dec. 15, 2023. [Online]. Available: https://www.bgpmon.net/bgp-leak-causing-internet-outages-in-japan-and-beyond/

[19] C. Villamizar, R. Chandra, and R. Govindan, “BGP route flap damping,” *RFC 2439*, 1998. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc2439/

[20] Z. M. Mao, R. Govindan, G. Varghese, and R. H. Katz, “Route flap damping exacerbates internet routing convergence,” in *Proc. 2002 ACM SIGSAC Conf. Comput. Commun. Secur.*, Pittsburgh, Pennsylvania, USA, 2002, pp. 221–233.

[21] A. Heffernan, “Protection of BGP sessions via the TCP MD5 signature option,” *RFC 2385*, 1998. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc2385/

[22] J. Touch, A. Mankin, and R. Bonica, “The TCP authentication option,” *RFC 5925*, 2010. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc5925/.

[23] M. Schuchard, A. Mohaisen, D. Foo Kune, N. Hopper, Y. Kim and E. Y. Vasserman, “Losing control of the Internet: Using the data plane to attack the control plane,” in *Proc. ACM Conf. Comput. Commun. Secur.*, Chicago, Illinois, USA, 2010, pp. 726–728.

[24] Y. Zhang, Z. M. Mao, and J. Wang, “Low-rate TCP-targeted dos attack disrupts internet routing,” in *Proc. 14th Annual Netw.. Distrib.. Syst. Secur. Symp.*, San Diego, USA, 2007, pp. 1–15.

[25] Y. Su, B. Wang, Q. Xing, P. Li, X. Wang and C. Li, "Research on blockchain-based inter-domain routing authentication technology," in *Proc. Conf. Commun. Tech.*, Tianjin, China, 2021, pp. 810–816.

[26] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (S-BGP)," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 4, pp. 582–592, 2000. doi: 10.1109/49.839934.

[27] N. Wang, X. H. Du, W. J. Wang, and A. D. Liu, "A survey of the border gateway protocol security," *Chin. J. Comput.*, vol. 40, no. 7, pp. 1626–1648, 2017.

[28] R. White, "Securing BGP through secure origin BGP (soBGP)," *Internet Protoc. J.*, vol. 3, no. 6, pp. 15–22, 2003.

[29] P. C. van Oorschot, T. Wan, and E. Kranakis, "On interdomain routing security and pretty secure BGP (psBGP)," *ACM Trans. Info. Syst. Secur.*, vol. 10, no. 3, pp. 1–41, 2007. doi: 10.1145/1266977.1266980.

[30] M. Lepinski and S. Kent, "An infrastructure to support secure internet routing," *RFC 6480*, 2012. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc6480/

[31] M. Lepinski, S. Kent, and D. Kong, "A profile for route origin authorizations (ROAs)," *RFC 6482*, 2012. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc6482/

[32] M. Lepinski and K. Sriram, "BGPSEC protocol specification," *RFC 8205*, 2017. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc8205/

[33] K. Shrishak and H. Shulman, "Limiting the power of RPKI authorities," in *Proc. 2020 Appl. Netw.. Res Work.*, Spain, 2020, pp. 12–18.

[34] Q. Li, J. Liu, Y. C. Hu, M. Xu, and J. Wu, "BGP with BGPsec: Attacks and countermeasures," *IEEE Netw.*, vol. 33, no. 4, pp. 194–200, 2019. doi: 10.1109/MNET.2018.1800171.

[35] D. Cooper, E. Heilman, K. Brogle, L. Reyzin, and S. Goldberg, "On the risk of misbehaving RPKI authorities," in *Proc. 12th ACM Work. Hot Top. Netw.*, College Park, MD, USA, 2013, pp. 1–7.

[36] R. Bush and R. Austein, "The resource public key infrastructure (RPKI) to router protocol," *RFC 6810*, 2013. Accessed: Dec. 15, 2023. [Online]. Available: https://datatracker.ietf.org/doc/rfc6810/

[37] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. Accessed: Dec. 15, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[38] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert. Syst. Appl.*, vol. 154, no. 10, pp. 1–21, 2020. doi: 10.1016/j.eswa.2020.113385.

[39] I. Gorkey, E. Sennema, C. El Moussaoui, and V. Wijdeveld, "Comparative study of byzantine fault tolerant consensus algorithms on permissioned blockchains," 2020. (Accessed: December 15, 2023). [Online]. Available: http://resolver.tudelft.nl/uuid:01083a4a-900b-4cf9-9746-cb9258c11d9e

[40] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982. doi: 10.1145/357172.357176.

[41] A. Hari and T. V. Lakshman, "The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet," in *Proc. 15th ACM Work. Hot Top., Netw.*, Atlanta, USA, 2016, pp. 204–210.

[42] Q. Q. Xing, B. S. Wang, and X. F. Wang, "BGPCoin: A trustworthy blockchain-based resource management solution for BGP security," in *Proc. 2017 ACM SIGSAC Conf. Comput. Commun. Secur.*, Dallas, TX, USA, 2017, pp. 2591–2593.

[43] Q. Q. Xing, B. S. Wang, and X. F. Wang, "BGPcoin: Blockchain-based internet number resource authority and BGP security solution," *Sym.*, vol. 10, no. 9, pp. 408–430, 2018. doi: 10.3390/sym10090408.

[44] J. Paillisse, M. Ferriol, and E. Garcia, "IPchain: Securing IP prefix allocation and delegation with blockchain," 2018. Accessed: Dec. 15, 2023. [Online]. Available: https://arxiv.org/abs/1805.04439

[45] S. Angieri, A. García-Martínez, B. Liu, Z. Yan, C. Wang and M. Bagnulo, "An experiment in distributed Internet address management using blockchains," 2018. Accessed: Dec. 15, 2023. [Online]. Available: https://arxiv.org/abs/1807.10528

[46] A. Garcia-Martinez, S. Angieri, B. Y. Liu, F. Yang, and M. Bagnulo, "Design and implementation of InBlock—A distributed IP address registration system," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3528–3539, 2021. doi: 10.1109/JSYST.2020.3003526.

[47] J. Li, M. V. Xu, J. H. Cao, Z. L. Meng, and G. Q. Zhang, "Decentralized Internet number resource management system based on blockchain technology," *J. Tsinghua Univ. (Sci. & Technol.)*, vol. 63, no. 9, pp. 1366–1379, 2023.

[48] A. de La Rocha Gómez-Arevalillo and P. Papadimitratos, "Blockchain-based public key infrastructure for inter-domain secure routing," in *Proc. Work. Open Problems. Netw. Secur.*, Rome, Italy, 2017, pp. 20–38.

[49] L. Mastilak, M. Galinski, P. Helebrandt, I. Kotuliak, and M. Ries, "Enhancing border gateway protocol security using public blockchain," *Sens.*, vol. 20, no. 16, pp. 1–11, 2020. doi: 10.3390/s20164482.

[50] I. Sfirakis and V. Kotronis, "Validating IP prefixes and AS-Paths with blockchains," 2019. Accessed: Dec. 15, 2023. [Online]. Available: https://arxiv.org/abs/1906.03172

[51] M. Saad, A. Anwar, A. Ahmad, H. Alasmary, M. Yuksel and A. Mohaisen, "RouteChain: Towards blockchain-based secure and efficient BGP routing," in *Proc. 2019 IEEE Int. Conf. Blockchain Crypto.,* Seoul, South Korea, 2019, pp. 210–218.

[52] D. Chen, Y. Ba, H. Qiu, J. Zhu, and Q. Wang, "ISRchain: Achieving efficient interdomain secure routing with blockchain," *Comput. Electr. Eng.*, vol. 83, no. 1, pp. 1–14, 2020. doi: 10.1016/j.compeleceng.2020.106584.

[53] G. B. He, W. Su, S. Gao, and J. Yue, "Securing route origin authorization with blockchain for inter-domain Routing," in *Proc. 2020 Conf. Work. Netw.*, Paris, France, 2020, pp. 504–508.

[54] G. B. He, W. Su, S. Gao, J. Yue, and S. K. Das, "ROAchain: Securing route origin authorization with blockchain for inter-domain routing," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1690–1705, 2021. doi: 10.1109/TNSM.2020.3015557.

[55] P. Podili, S. R. Cherupally, S. Boga, and K. Kataoka, "Inter-domain prefix and route validation using fast and scalable DAG based distributed ledger for secure BGP routing," *J Netw. Syst. Manag.*, vol. 30, pp. 55, 2022.

[56] H. M. Lu, Y. Tang, and Y. Sun, "DRRS-BC: Decentralized routing registration system based on blockchain," *IEEE/CAA J. Autom. Sin.*, vol. 8, no. 12, pp. 1868–1876, 2021. doi: 10.1109/JAS.2021.1004204.

[57] I. W. Budi Sentana, M. Ikram, and M. Ali Kaafar, "BlockJack: Towards improved prevention of Ip prefix hijacking attacks in inter-domain routing via blockchain," in *Proc. 18th Int. Conf. Secur. Cryptogr. SECRYPT 2021*, 2021, pp. 674–679.

[58] Y. P. Liu *et al.*, "A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks," *J. Parallel. Distrib. Comput.*, vol. 142, no. 1, pp. 77–89, 2020. doi: 10.1016/j.jpdc.2020.04.005.

[59] M. F. Galmes, R. Coll Aumatell, A. Cabellos-Aparicio, S. Ren, X. Wei and B. Liu, "Preventing route leaks using a decentralized approach," in *Proc. 2020 Int. Federat. Inf. Process. (IFIP) Netw. Conf.*, Paris, France, 2020, pp. 509–513.

[60] J. R. Yue, Y. J. Qin, S. Gao, W. Su, G. He and N. Liu, "A privacy-preserving route leak protection mechanism based on blockchain," in *Proc. 2021 IEEE Int. Conf. Inf. Commun. Softw. Eng.*, Chengdu, China, 2021, pp. 264–269.

[61] D. Chen, H. Qiu, J. H. Zhu, Q. X. Wang, and S. W. Fan, "Blockchain-based validation method for inter-domain routing policy compliance," *J. Softw.*, vol. 34, no. 9, pp. 4336–4350, 2023.

[62] X. Deng, K. Li, Z. Wang, J. Li, and Z. Luo, "A survey of blockchain consensus algorithms," in *Proc. 2022 Int. Conf. Blockchain Tech. Inf. Sec. (ICBCTIS)*, Huaihua, China, 2022, pp. 188–192.

[63] W. Zhong *et al.*, "Byzantine fault-tolerant consensus algorithms: A survey," *Electron.*, vol. 12, no. 18, pp. 1–25, 2023.