Grenze International Journal of Engineering and Technology, June Issue

Enhancing Border Gateway Protocol Security using Public Blockchain

Shipra Shukla[1], Swastika Gupta[2], Misha Rai[3], Muskan Bhati[4] and Vanshika Chaudhary[5]
[1-5]Dept. of CSE, AUUP
Email: ershiprashukla88@gmail.com, swastikagupta67@gmail.com, misharai2001@gmail.com, muskanbhati712@gmail.com, vanshikavv2@gmail.com

***Abstract*—The Border Gateway Protocol (BGP) is the backbone of the internet, responsible for routing traffic between autonomous systems (AS). BGP is essential for maintaining the integrity and stability of the internet. However, the trust-based nature of BGP makes it vulnerable to a range of attacks, such as route hijacking, route leaking, and BGP prefix spoofing. These attacks can result in traffic being redirected to unauthorized destinations, leading to security breaches, loss of data, and even financial losses. To address these vulnerabilities, researchers and industry experts have proposed various solutions, including those based on centralized Public Key Infrastructure (PKI). However, these solutions have their own set of challenges, including slow adoption rates, high costs, and susceptibility to attacks. One promising solution is the use of public blockchain technology, which offers a decentralized, transparent, and secure way to verify and validate BGP updates. Public blockchains, such as Bitcoin and Ethereum, rely on a consensus mechanism to validate transactions and maintain the integrity of the network. By leveraging the consensus mechanism, BGP updates can be verified and validated in a trust-less manner, reducing the risk of attacks. Using a public blockchain for BGP also enables transparency and auditability, which are crucial for detecting and preventing attacks. The blockchain maintains an immutable record of all BGP updates, providing a verifiable history of changes. This allows network administrators to review router settings and detect false information broadcasts, which can be invaluable in identifying and mitigating attacks. One approach to using blockchain for BGP security is to implement a decentralized system for verifying BGP updates, such as the Border Gateway Protocol Security with Blockchain (BGPSB) proposed by researchers. This system uses a smart contract to validate BGP updates and prevent prefix spoofing. The smart contract is deployed on a public blockchain, providing a transparent and auditable way to verify BGP updates. In conclusion, the use of public blockchain technology has the potential to enhance the security of BGP routing. By leveraging the decentralized, transparent, and secure nature of blockchain, BGP updates can be verified and validated in a trust-less manner, reducing the risk of attacks. This, in turn, can help maintain the integrity and stability of the internet, which is essential for our increasingly connected world.**

***Index Terms*— Border Gateway Protocol, BGP hijacking, BGP security, Blockchain, Public Blockchain, management, network.**

I. INTRODUCTION

The internet is made up of many autonomous systems (AS) that communicate with each other using [1] (BGP) to

Grenze ID: 01.GIJET.9.2.552

share routing information. However, Autonomous Systems trust each other by default, which can leave them vulnerable to BGP hijacking attacks where a malicious actor reroutes. The trust-based nature of BGP makes it vulnerable to various attacks, such as BGP hijacking, route leaking, and prefix spoofing. BGP hijacking is one of the most common types of attacks that attackers use to manipulate internet traffic. This type of attack occurs when an attacker maliciously takes over a network's IP address and uses an autonomous system to redirect internet traffic for that network. This is done by claiming false ownership of IP addresses and announcing them through a malicious Autonomous System. It is like, changing the signage on a freeway to redirect traffic to the wrong exit. By doing so, attackers can access sensitive information, disrupt services, or launch further attacks. While technologies have been developed to prevent these attacks, they are difficult to deploy and have not yet been widely adopted. To prevent such attacks, various solutions have been proposed, such as centralized Public Key Infrastructure (PKI) and Resource Public Key Infrastructure (RPKI). However, these solutions have their own limitations, including slow adoption and vulnerability to attacks. Decentralized solutions based on blockchain technology have emerged as a potential solution to enhance the security of BGP [1].

Blockchain is a decentralized, digital ledger that records transactions in a secure, tamper-proof manner. It stores data in a series of records called blocks, which are linked together using cryptography. Each block contains a unique digital signature, or hash, that identifies the block and its contents. When a new block is added to the chain, it contains information about the previous block, including its hash. This creates an unbroken chain of blocks, with each block connected to the one before it. This makes it extremely difficult to alter or tamper with the information stored in the blockchain, as any change to a single block would break the entire chain. Blockchain technology is particularly useful for recording and verifying transactions in a transparent and secure way. Because the ledger is decentralized and publicly accessible, it provides a high degree of trust and accountability, as anyone can view the records and verify the transactions. This makes it especially useful for applications such as financial transactions, supply chain management, and digital identity verification.

Border Gateway Protocol [1] is a gateway protocol used to exchange routing information among autonomous systems (AS) on the internet. Autonomous systems are networks that are managed by a single administrative entity and have a unique numeric identifier called an autonomous system number (ASN). BGP enables the autonomous systems to communicate with each other and share routing information, which is essential for the internet to function effectively. BGP is designed to provide stable and reliable routing in the face of network failures and changes. It is a path-vector protocol, which means that it selects the best path to a destination based on a set of policies or rules that are established by the network administrators. The policies can be based on factors such as network performance, cost, or security. BGP routers maintain a routing table that contains information about the network topology and the paths to other networks. Each router sends updates to its neighbors about the changes in the routing table, and the neighbors, in turn, propagate the updates to their neighbors until all routers have the latest routing information. BGP routers establish peering relationships with other routers in the same autonomous system or in other autonomous systems to exchange routing information. BGP uses a client-server topology to transmit routing information. A BGP [1] session is initiated by a client router that sends queries to a server router, requesting updates to the routing table. The server responds by sending the requested updates, and the client updates its routing table accordingly. BGP sessions can be established using different transport protocols such as TCP or UDP. One of the challenges of BGP is that it is vulnerable to attacks based on false information. Malicious parties can send false routing information to a BGP router, which can result in routing loops, blackholes, or BGP hijacking. BGP hijacking occurs when an attacker announces a false prefix to a BGP router, causing the traffic to be routed through the attacker's network. BGP hijacking is a serious security threat, as it can be used for traffic interception, eavesdropping, or data manipulation. In conclusion, BGP is a critical protocol that enables the internet to function by providing stable and reliable routing among autonomous systems. It is designed to select the best path to a destination based on network policies and can handle network failures and changes. However, BGP is vulnerable to attacks based on false information, and network administrators should take appropriate measures to protect their networks from such attacks [2].

There are two flavors of BGP:

External BGP (eBGP) - External Border Gateway Protocol is referred to as eBGP. Routing data is exchanged between autonomous systems to other autonomous systems via external BGP. In order to connect two or more autonomous systems, it is used and deployed on edge or border routers. It acts as the protocol in charge of connecting diverse networks or organisations to the Internet. For eBGP, the administrative separation is 20.

Internal BGP (iBGP) - Internal Border Gateway Protocol is referred to as iBGP. Using internal BGP, an autonomous system can communicate routing details with other autonomous systems. Your internal router

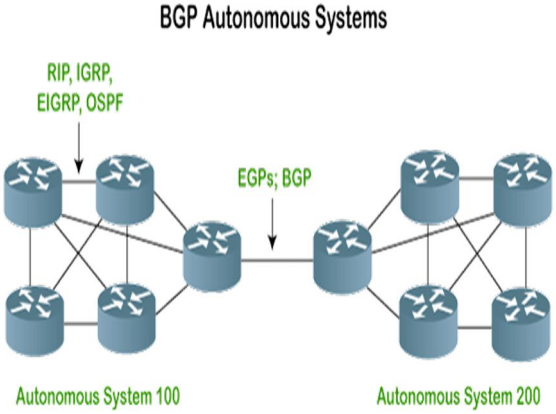


Figure 1

receives information from it. To create a route reflector and federation using the full mesh topology or prefix learning, the entire autonomous system's equipment is required. For iBGP, the administrative separation is 200.
Three different types of routing tables are used by BGP-enabled routers for various purposes:
Neighbour Table - a table with details about BGP neighbours. This includes neighbours that the administrator has manually set up. The Neighbour command must be used to manually configure the neighbour relationship. It is used to verify with the command:
#show ip bgp neighbours
#show ip bgp summary
Forwarding Table: You may confirm this contains all routes listed in BGP by running the command:
display ip bgp
IP Routing Table: The most effective routes needed to get to the destination are listed in the IP routing table. The optimal routing path is displayed using the following command when BGP determines it is the best one for the network:
ip route #SH
We propose a solution to increase the level of BGP routing security with the blockchain. In the proposed structure, we not only verify received BGP ads like BGP Coin, but we also avoid learning fake prefixes. Our contributions are:
1.The addition of a technique to enable routers with AS to automatically discover every prefix assigned to AS. By doing this, we stop routers from promoting prefixes with their AS origin if they haven't been given to an Autonomous System.
2.We use the open blockchain to create our proof of concept architecture. Based on the number of prefixes per transaction, we estimate the time and cost needed to update routing information using the measured results.

II. Objective

If one internet path goes down, BGP preserves network stability by ensuring that routers can swiftly react to transmit packets through a different channel. Based on pathways, rules, or network policies set up by a network administrator, BGP decides where to route traffic. A common routing table is kept by each BGP router and is used to steer packets while they are in transit. BGP communicates routing information via a client-server topology. The client-server starts a BGP session by making a request to the server. AS generally have trust for one another and think their neighbour is advertising accurate information. This practise is a little naive because it leaves room for future attacks by considering all incoming BGP advertising as real and proper. BGP attacks are one of the most frequent types of BGP attacks. An autonomous system (AS) controlled by a hostile actor aims to steal a network's IP address and reroute traffic for this network. By producing a record that cannot be altered and is end-to-end encrypted, blockchain contributes to the prevention of fraud and unlawful conduct. Since the data is kept on a network of computers rather than a server, it is more exposed to hackers and challenging to access or modify. Blockchain uses a distributed ledger, in which identical records of transactions and data are kept across numerous sites. Full transparency is provided since every network user with permissions can see the same data at once. Blockchain establishes an audit trail that records an asset's emergence at each stage of its path. Traditional paper-intensive procedures take time, human error-prone and frequently call for third-party mediation. Blockchain enables transactions to be done more quickly and effectively. We suggest using the blockchain to improve the security of BGP routing. In the suggested structure, we avoid learning bogus prefixes and not merely check received BGP advertising like BGP Coin [2].

III. Literature Review

1. Vincenzo Morabito - It's crucial to stay informed about technological advancements, including blockchain. Five key concepts of blockchain - smart contracts, decentralized consensus, blockchain, trusted computing, and proof of work/stat - must be understood and how they relate to each other for its potential to be fully realized.

2. Gavin Smith - Distributed ledger technology has emerged from the lab and is now on the c-suite agenda of various clients, from startups to multinational giants. It has the potential to transform economics, business, and practice, and businesses must understand its workings, potential applications, and interaction with the legal framework.
3. Tao Wan and all - BGP is the primary routing protocol used on the Internet, responsible for discovering and maintaining routing information for transmitting traffic across the network. As a critical component of the Internet infrastructure, BGP attacks can cause significant service disruptions. This paper examines BGP protocol operations, security vulnerabilities, threats, and mechanisms.
4. Ben Piper - This paper emphasizes the significance of Border Gateway Protocol (BGP) in maintaining the Internet infrastructure for over 30 years. BGP, developed as the successor of External Gateway Protocol (EGP), is widely used due to its flexibility and extendibility, with many organizations implementing it internally.
5. Dmitri Tsumak - BGP is a fundamental routing protocol used between autonomous systems on the Internet, but it lacks security measures and needs additional tools and protocols to manage it. Various security solutions were introduced to address its security concerns. A new solution that utilizes blockchain technology and smart contracts is also suggested to facilitate message verification among peers.
6. Beny Nugraha and all - BGP is crucial for routing information between AS on the Internet but is highly vulnerable to security issues, such as prefix hijacking. Filtering can mitigate this vulnerability by ensuring that prefixes are obtained from and advertised only to trusted BGP peers.
7. Nikhil Hemant Bhagat - This paper presents a comparison between different protocols using diagrams and tables for reference. The practical application of the issues is demonstrated, and it is suggested that BGP should be used only for external routing and not internal routing.
8. Prof Dr Aftab Malik and all - This paper analyzes the critical technology behind digital communication using Internet or IOT technologies and the protocols used by routers. It specifically focuses on the Border Gateway Protocol, discussing its types, features, security threats, and risks.
9. Zibin Zheng - This paper offers a thorough review of blockchain technology, highlighting its immutable ledger capabilities and decentralized transaction capabilities. The architecture of blockchain is outlined, and several common consensus algorithms used in various blockchain systems are compared. Technical obstacles and recent developments are briefly discussed. The study concludes with a look at potential future blockchain trends.
10. Min Xu and all - This study examines academic research on blockchain in the fields of business and economics, identifying five main research topics: economic benefits, blockchain technology, initial coin offerings, the fintech revolution, and the sharing economy. A clustering analysis is conducted to group the research into these categories.
11. Zhiwei Yan - Proposing a novel management architecture for BGP, this article introduces BGP Chain, a blockchain-based solution to mitigate the security threats of BGP. As BGP was originally designed without sufficient security considerations, it has become vulnerable to various security issues. BGP Chain aims to establish a secure, smart, and agile routing infrastructure for the future Internet.

IV. Design

Figure 2 illustrates the proposed BGP Chain architecture consisting of two interconnected modules. The first module focuses on securely transferring configuration files to the router through a blockchain network. The second module provides a reliable approach for protecting against IP prefix hijacking by checking the Route Origin Authorization (ROA) data of each IP prefix in a blockchain. This prevents the acceptance of unauthorized IP prefixes but does not prevent their propagation. To address this issue, the architecture proposes an approach where routers advertise only approved prefixes in BGP update messages. This involves downloading the blockchain network's IP prefixes and verifying that they are legitimate before including them in the update message. This ensures that only authentic IP prefixes are advertised through BGP and prevents both malicious and accidental misconfigurations. However, this approach does not affect the spread of prefixes obtained from nearby Autonomous Systems.

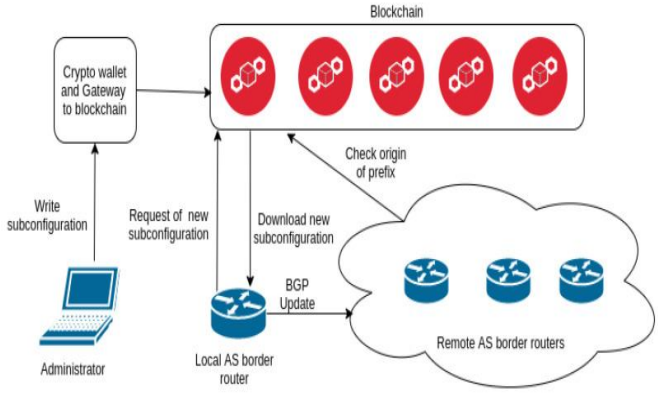
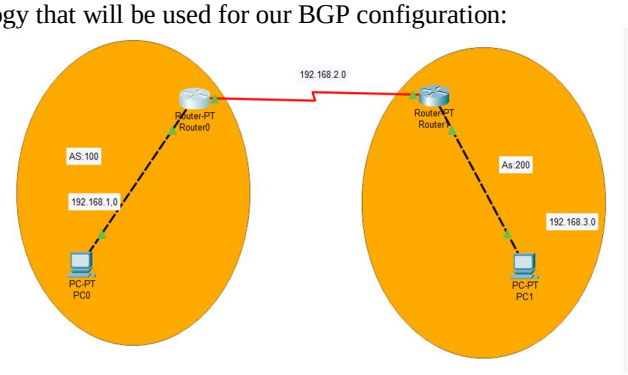


Figure 2

BGP configuration Example 1:

A straightforward Packet Tracer BGP Configuration example will be made in order to better grasp BGP (Border Gateway Protocol). Two AS (Autonomous Systems), each with a computer and a router, will be used in the arrangement.

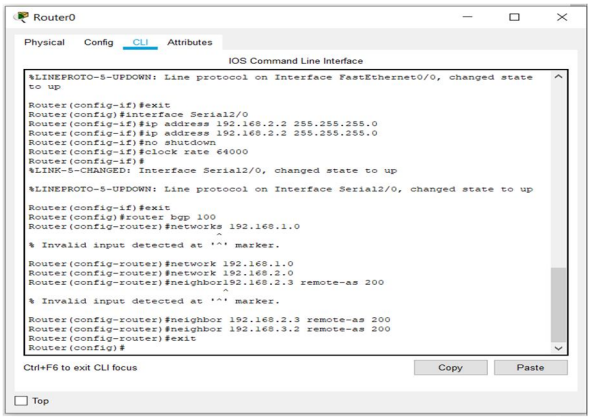
The following is the topology that will be used for our BGP configuration:



For **BGP Configuration**, we need to configure the IP addresses of interfaces as other examples.

For Router 0:

Router (config-if) #exit
Router (config) #router bgp 100
Router (config-router) #network 192.168.1.0
Router (config-router) #network 192.168.2.0
Router (config-router) #neighbor 192.168.2.3 remote-as 200
Router (config-router) #neighbor 192.168.2.3 remote-as 200
Router (config-router) #neighbor 192.168.3.2 remote-as 200
Router (config-router) #exit
Router (config) #



For Router 1:

Router (config-if) #exit
Router (config) #router bgp 200
Router (config-router) #network 192.168.2.0
Router (config-router) #network 192.168.3.0
Router (config-router) #neighbor 192.168.2.2 remote-as 100
Router (config-router) #neighbor 192.168.1.2 remote-as 100
Router (config-router) #exit
Router (config) #

BGP configuration Example 2:

We'll create a straightforward Packet Tracer BGP Configuration example to help you better grasp BGP (Border Gateway Protocol). Two AS (Autonomous Systems) will be used in the arrangement, each with a computer and a router.

The topology that we'll utilise for our BGP configuration is as follows:

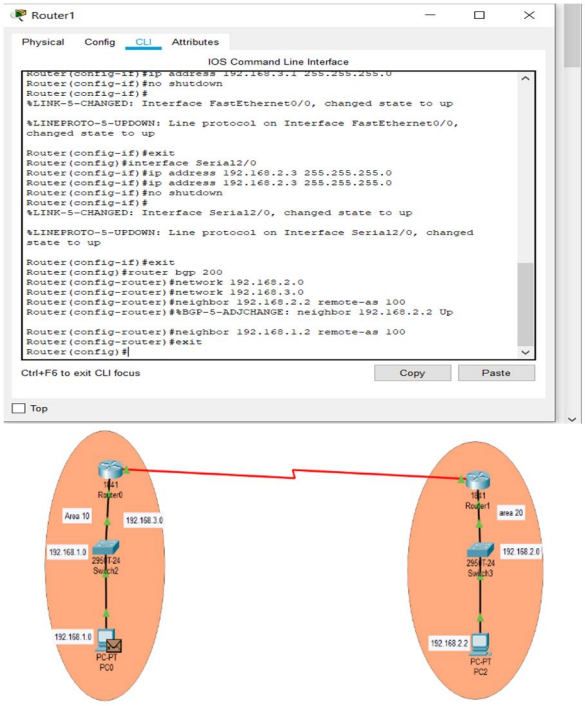


Fig: Message from pc0 is send to pc2

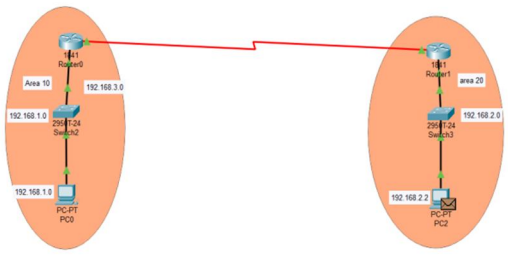
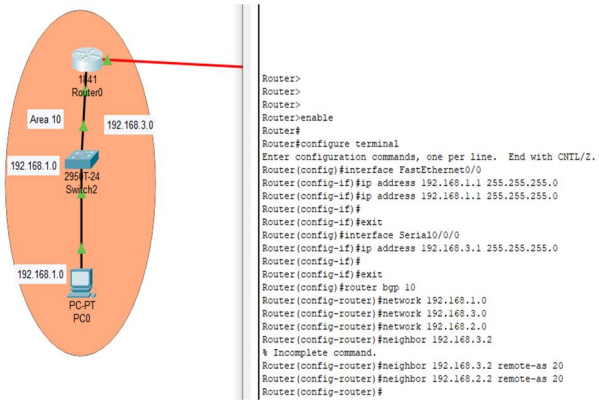
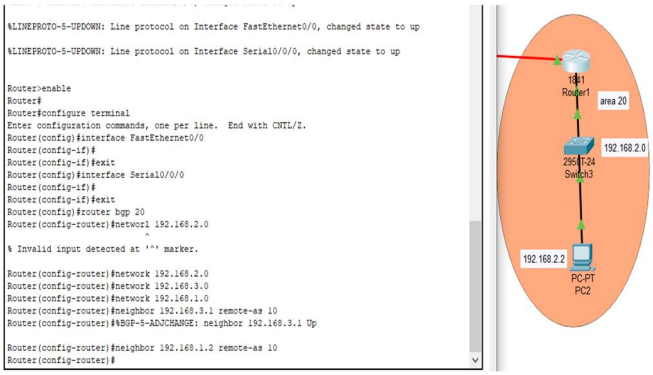


Fig: Message sent by pc0 is received by pc2

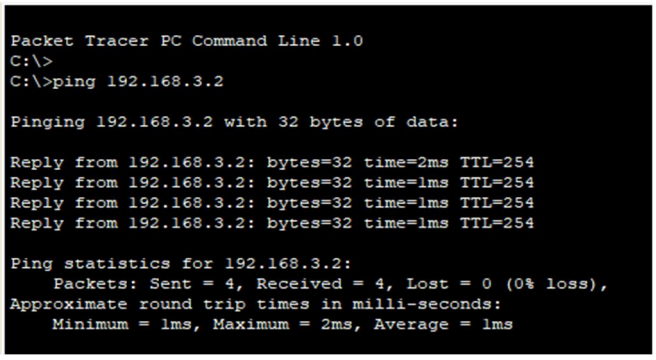
For **BGP Configuration**, we need to configure the IP addresses of interfaces:
Router (config-if) #exit
Router (config) #router bgp 10
Router (config-router) #network 192.168.1.0
Router (config-router) #network 192.168.3.0
Router (config-router) #network 192.168.2.0
Router (config-router) #neighbor 192.168.3.2 remote-as 20
Router (config-router) #neighbor 192.168.2.2 remote-as 20

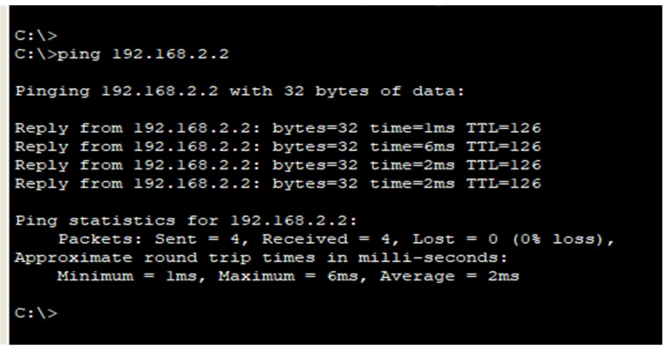


Router (config-if) #exit
Router (config) #router bgp 20
Router (config-router) #network 192.168.2.0
Router (config-router) #network 192.168.3.0
Router (config-router) #network 192.168.1.0
Router (config-router) #neighbor 192.168.3.1 remote-as 10
Router (config-router) #neighbor 192.168.1.2 remote-as 10



Ping Command in command prompt:
Ping 192.168.3.2
Ping 192.168.2.2





V. IMPLEMENTATION

The implementation of enhancing BGP using public blockchain security involves several steps. Here are some of the key steps:

1.Setting up a Public Blockchain: The first step in implementing BGP security using public blockchain is to set up a blockchain network. The blockchain network must be public, decentralized, and secure to ensure that the information stored on the blockchain is tamper-proof and immutable. Ethereum, for example, is a popular public blockchain that is decentralized and secure.

2.Creating Smart Contracts: Smart contracts are self-executing computer programs that are stored on the blockchain. In the case of BGP security, smart contracts can be used to define the rules and conditions for validating BGP routes. The smart contracts can be written in Solidity, a programming language used to write smart contracts on the Ethereum blockchain.
3.Registering Autonomous Systems (AS) on the Blockchain: The next step is to register Autonomous Systems (AS) on the blockchain. Each AS can register its own routes on the blockchain, and the routes will be stored in the smart contract. The registration process involves providing information about the AS, such as its name, IP address range, and BGP router information.
4.Validating BGP Routes: After AS registration, other AS can validate the legitimacy of the routes they receive from their peers. The validation process involves querying the smart contract to verify that the routes are registered by legitimate AS and that they are not malicious.
5.Monitoring BGP Routes: The blockchain can also be used to monitor BGP routes and detect any anomalies or attacks. This can be done by setting up a node on the blockchain network that listens to BGP announcements and compares them to the routes registered on the blockchain.
6.Alerting System: If an anomaly or attack is detected, an alerting system can be triggered to notify the relevant parties. The alerting system can be set up to send alerts via email, SMS, or other communication channels.
In a blockchain, each block contains a unique digital fingerprint, called a hash, which is generated using a cryptographic hash function. This hash is based on the data contained within the block, and any changes to the data will result in a different hash value. The hash of each block is included in the header of the next block in the chain, creating a linked list of blocks. The linking of blocks in a blockchain creates an unalterable and tamper-proof record of all the transactions on the network. If anyone tries to modify the data in a block, it will result in a different hash value, which will not match the hash value stored in the header of the next block. This discrepancy will alert the network to the attempted tampering, making it extremely difficult to modify or corrupt the blockchain.
To implement a blockchain using Python, we can use data structures like lists and dictionaries to store the blocks and transactions, and hash functions like SHA-256 to create and validate block hashes. The implementation involves creating classes to represent the blockchain, blocks, and transactions. Each block contains a hash that is based on the data in the block and the hash of the previous block in the chain. To add new blocks to the chain, we need to validate the integrity of the chain by checking the hash of the previous block against the one stored in the new block. By implementing a blockchain using Python, we can gain a deeper understanding of how this technology works and its potential applications in various industries. Blockchain technology can provide a secure and transparent way to store and verify data, making it valuable in fields such as finance, supply chain management, and healthcare. Understanding the basics of blockchain implementation can also help developers to create new and innovative applications using this technology.

VI. CONCLUSION

As was mentioned in the introduction, there are some security flaws with BGP. Prefixes can be taken over to change how traffic is routed. We changed the original architecture to work with edge routers of ASes to strengthen defence against this attack. For prefixes assigned to an AS, our updated architecture offers decentralised and immutable storage. Finally, we have put in place a collection of smart contracts to control the BGP configurations for the AS's edge routers. Our approach reduces the quantity of fake BGP origin announcements by enabling prefix verification prior to dissemination to routers. Additionally, it utilises blockchain to maintain a complete record of all modifications. Reactive prefix information verification of BGP update packets is the focus of related blockchain-based research. The primary innovation of our approach is that we prioritise proactive fraud prevention of BGP origin announcements over reactive BGP origin AS validation. We accomplish this by deploying configurations that may be verified as correct to routers in the origin AS. We wish to concentrate our research in the future on a different setting for this architecture. In order to get results that are more applicable to the vast scope of the Internet, we wish to test this design in more complex topologies. A longer list of BGP properties should be considered in future developments with the goal of decreasing assaults on BGP by following the AS pathways. The transaction could be improved by including details about ties to other peers. Additionally, we want to improve the way the existing implementation checks for AS updates on a regular basis. Sending notification messages after pertinent changes have spread throughout the blockchain could take the role of this approach. The most recent enhancement to the architecture that we know of is a more effective consensus-building formula. Currently, Proof of Work is used in implementation. We could reduce the uploading sub-duration configuration's time if we replaced it.

REFERENCES

[1] https://www.sciencedirect.com/science/article/abs/pii/S0045790617321390
[2] https://www.igi-global.com/gateway/article/240252#pnlRecommendationForm
[3] Mitseava A., Panchenko A., Engel T. The state of affairs in BGP security: A survey of attacks and defenses. Comput. Commun. 2018;**124**:45–60. doi: 10.1016/j.comcom.2018.04.013. [CrossRef] [Google Scholar]
[4] Lepinski M., Sriram K. BGPsec Protocol Specification. [(accessed on 5 August 2020)]; Available online: https://www.hjp.at/doc/rfc/rfc8205.html
[5] Lepinski M., Kent S. An Infrastructure to Support Secure Internet Routing. [(accessed on 5 August 2020)]; Available online: https://www.hjp.at/doc/rfc/rfc6480.html
[6] Arslanian H., Fischer F. The Future of Finance. Palgrave Macmillan; Cham, London, UK: 2019. Blockchain As an Enabling Technology; pp. 113–121. [Google Scholar]
[7] Lai R., Chuen D.L.K. Handbook of Blockchain, Digital Finance, and Inclusion. Volume 2. Academic Press; Cambridge, MA, USA: 2018. Blockchain—From public to private; pp. 145–177. [Google Scholar]
[8] Helebrandt P., Belluš M., Ries M., Kotuliak I., Khilenko V. Blockchain Adoption for Monitoring and Management of Enterprise Networks; Proceedings of the 2018 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON); Vancouver, BC, Canada. 1–3 November 2018; pp. 1–5. [Google Scholar]
[9] Xing Q., Wang B., Wang X. BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution. Symmetry. 2018;**10**:408. doi: 10.3390/sym10090408. [CrossRef] [Google Scholar]
[10] Saad M., Anwar A., Ahmad A., Alasmary H., Yuksel M., Mohaisen A. RouteChain: Towards Blockchain-based Secure and Efficient BGP Routing; Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); Seoul, Korea. 14–17 May 2019; pp. 210–218. [Google Scholar]
[11] Hari A., Lakshmaan T.V. The internet blockchain: A distributed, tamper-resistant transaction framework for the internet; Proceedings of the 15th ACM Workshop on Hot Topics in Networks; Atlanta, GA, USA. 16 November 2016; pp. 204–210. [Google Scholar]
[12] Ma X., Xu D., Dang H. BGP-LSChain: An Inter-domain Link State Sharing Framework Based on Blockchain; Proceedings of the 2019 International Conference on Blockchain Technology; Honolulu, HI, USA. 15–17 March 2019; pp. 19–23. [Google Scholar]
[13] Shapira T., Shavitt Y. A Deep Learning Approach for IP Hijack Detection Based on ASN Embedding; Proceedings of the Workshop on Network Meets AI & ML, Virtual Event; New York, NY, USA. 23 August 2020; pp. 35–41. [Google Scholar]
[14] McGlynn K., Acharya H.B., Kwon M. Detecting BGP Route Anomalies with Deep Learning; Proceedings of the 2019 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); Paris, France. 29 April–2 May 2019; pp. 1039–1040. [Google Scholar]
[15] Martinez-Garcia M., Zhang Y., Suzuki K., Zhang Y.D. Deep Recurrent Entropy Adaptive Model for System Reliability Monitoring. IEEE Trans. Ind. Informatics. 2020 doi: 10.1109/TII.2020.3007152. [CrossRef] [Google Scholar]
[16] Košťál K., Helebrandt P., Belluš M., Ries M., Kotuliak I. Management and Monitoring of IoT Devices Using Blockchain. Sensors. 2019;**19**:856. doi: 10.3390/s19040856. [PMC free article] [PubMed] [CrossRef] [Google Scholar]
[17] Rekhter Y., Tony L., Susan H. A Border Gateway Protocol 4 (BGP-4) [(accessed on 5 August 2020)]; Available online: https://www.hjp.at/doc/rfc/rfc4271.html
[18] Ubuntu Server 20.04 LTS. [(accessed on 3 August 2020)]; Available online: https://releases.ubuntu.com/20.04/
[19] Ma J. Gwei. [(accessed on 3 August 2020)]; Available online: https://academy.binance.com/glossary/gwei