Grenze International Journal of Engineering and Technology, June Issue

Security using Blockchain in BGP Protocol

Avi Chakravarti[1] and Shipra Shukla[2]
[1]Department of CSE, Amity School of Engineering and Technology, AUUP, Noida, UP, India
Email: avichakravarti3@gmail.com
[2]Assistant Professor, Department of CSE, Amity School of Engineering and Technology, AUUP, Noida, UP, India
Email: ershiprashukla88@gmail.com

***Abstract*—In the present Internet, the most fundamental infrastructure - The Border Gateway Protocol (BGP) supports the inter-connectivity of different Autonomous Systems (ASs) in which Multiple connections exist to external AS's through the same provider, but connect via a separate CO or routing policy and then the reachability between the devices can be accomplished from any network in the Net. Nevertheless, due to the absence of protection factor to consider throughout its initial stage, the BGP struggles with multiple safety dangers which ultimately results right into huge losses which is experienced in the past. One more obstacle is that it cannot sustain the future innovative applications with complex problems arising and with deterministic directing. In this research paper a novel BGP monitoring style, specifically BGPBlockChain, which is based upon the blockchain, and the algorithms used to build a secure network in order to develop a protected, wise, and nimble transmitting framework that is efficient enough to handle the new attacks from the malicious person over the network to steal and misuse the sensitive data and which creates a secured inter-connectivity vision as well as for the future Web.**

***Index Terms*— Border Gateway Protocol, blockchain, BGPBlockchain.**

I. INTRODUCTION

The web includes a huge set of networks known as autonomous systems (ASs), determined by serial number called AS numbers (ASNs). Every single AS consists of a variety of hosts and also routers under the management control of a single entity. ASs are granted a set of handed over IP addresses, which are, subsequently, designated to their hosts as well as routers. Each AS is responsible for forwarding traffic a minimum of to and from its IP addresses. To do this, ASs are linked via committed web links as well as bargain reachability info utilizing Border Gateway Protocol (BGP). Nevertheless, BGP routers accept any type of advertisements started by the network by default. However because of this protection problem it easily results in a serious Web safety and security threat called "route hijacking"[1]. It has a significant move on the regular operation of the network, which may result in routing great voids, web traffic eavesdropping and also large-scale refusal and also rejection of service strikes, etc

This was the main reason the Internet Engineering Task Force (IETF) has to proposed a numerical Resources Public Key Infrastructure (RPKI) to protect BGP route hijacking. In RPKI organization of Certification Authorities (CAs) in a hierarchical structure that is always aligned with the existing Internet Number Resources (INR) which includes the IP prefixes and AS numbers allocation hierarchy of the network in an Autonomous system. Each INR allocation requires a corresponding resource certificates to attest to it. The two important

Grenze ID: 01.GIJET.8.2.16_1
© Grenze Scientific Society, 2022

resource certificates which are needed during this above mentioned allocation process are: CA certificates and End Entity (EE) certificates. CA certificates are used to support attestations about the INR holdings, whereas EE certificates are primarily used for the validation of Route Origin Authorizations (ROA) that are used to verify if an AS is permitted to originate routes to specific IP prefixes [2].
An architecture for an infrastructure to support improved security of Internet routing is being discussed and it was laid by RKPI representing the allocation of IP addresses It encompasses 3 main principles:

- Resource Public Key Infrastructure (RPKI)
- Digitally signed routing objects to support routing security
- A distributed repository system to hold the PKI objects and the signed routing objects

The role of this architecture is to attest the certificates of other blocks to provide integrity and keep the record of all the entities by all the blocks[3].
A basic architecture was standardized mainly for RPKI that has a long series of Request for Comments (RFCs) which include: the chosen protocol to deliver the prefix from origin to the data routers. RKPI repository data protocol for data synchronization, algorithm procedure of RKPI and BGPsec which is developed to protect the BGP path security. But still there are number of unsatisfied problems when RKPI-a centralized structure is used with blockchain technology which will be a decentralized structure.

II. Literature Review

In the last decades survey provided a review in the area of BGP security solutions but it covered only some issue and later a broad overview was presented. In the initial era researchers discussed about BGP session attacks categorizing their impact on the distributed BGP routing system and what all difficulties are faced by the normal during these attacks as they make routing system get reset and while regaining the AS path unknown sources are added and trigger their cut off frequencies due to which a lot of service providing company faces penalties and represented the analytical model for these peering session attacks which results into slow connectivity at some areas and a loss of data and thus introduced various models of attacks and how these kind of attacks are done on various topologies [1][17].
Butler et al purposed the most comprehensive survey to make BGP secure in 2010. A similar kind of work was also done by Huston et al and covered BGP security extensions reflecting the start of art which was done almost twelve years ago but because of complex role of BGP over the Net, it was always prone to various attacks[4][5][6] .Even recently a standardization efforts made by IETF was reviewed by Siddique et al on Secure Inter-Domain Routing Working Group to secure BGP but focussed on less extension. Al-Musawi et al presented his views on various techniques to find cyber threats to BGP which include DDoS but didn't reviewed for mitigation and solutions[7].
In 2018 Thomas Angels discussed about BGP vulnerabilities and the kind of attacks which are performed on BGP and still there is an insight that the system is still vulnerable to many other attacks which can come to know in the future which makes it the most important topic of research as it is being used by all over the world and still there are lot of loop holes in its security. They also discussed about the properties which are required to secure BGP and also represented methodologies to update the existing methods of security discussing about all the other researchers approaches for making BGP secure and the detection recovery and mitigation systems through which can degrade the attack vectors [1][16].
Recently in the paper for Blockchain Inter Domain latency, the author proposes future internet architecture consisting of multiple AS which gives a brief description on how to provide latency aware routing in software defined network (SDN). Latency measurement results of the experiments are securely stored in distributed decentralized blockchain network where all AS holds its share and power. Each AS hosts is given it's SDN instance for interconnection with the neighbouring SDN controllers over AS border in the network. It instances processes latency measurement data from blockchain network and the validation of data integrity and manages latency aware routing for real-time data flows. After storing RTT values then takes the final step of validation processes which validates two-side data integrity for anomalies and advertises inter-AS RTT results to SDN for latency-aware routing decision[8].
The IETF proposed RKPI protocol has been talked about which was introduced for making BGP more secure but it lead to various loop holes which made BGP more vulnerable yet to various attacks such as BGP hijacking leading to tampering and DoS attacks[2]. The main operation of RPKI for verifying the route origin and making a secure environment for BGP was:

- CAs publish the authoritative objects into their repositories.

- Relying Parties2 (RPs) collect and verify their RPKI digital objects from the repositories and store the trustful results in their local caches.
- BGP routers use RP's verified results to check the route origin information contained in the received BGP message.

But still there were threats to RKPI which included Data production, Data synchronization and Data usage[2]. The repository system is structured as a distributed database, it should be inherently resistant to denial-of-service attacks; nonetheless, appropriate precautions should also be taken, both through replication and backup of the constituent databases and through the physical security of database servers[3].

III. BLOCKCHAIN FEATURES

In the emerging era of technology a ground breaking innovation named blockchain is being used as the enhancement of past technologies in a more secure way in various sectors of the technology [9]. It is a distributed, shared and secured ledger which helps the humans to track and keep the record of the resources without requiring centralized authority. Satoshi Nakamoto proposed Bitcoin with the potential application of blockchain which has helped to advance the security of financial assets. It is used to facilitate communication and exchange of resources among two parties in a network (P2P) without involving any administrator or central authority. All the communication takes place in anonymous form[10].

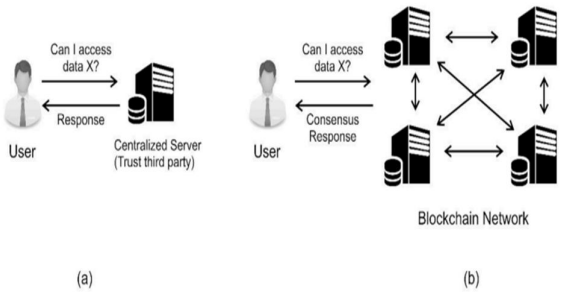

Figure 1.Blockchain design

It can be viewed Blockchain as log in which all its records are arranged in the form of timestamped blocks and all these blocks are uniquely identified by their cryptographic hash and every block references the hash of its previous node's hash. It helps in order to get the authenticity and timestamped network activity of the shared blockchain[11].

It can be utilized for smart contracts also as it ensure the trust mechanism which is established through transaction verification and when these transactions reaches consensus among all nodes the contents in the contract cannot be tampered. The core underlying technology of using blockchain includes: P2P network protocol, cryptographic encryption, data structure model, smart contract etc. Presently all the open source code based on above fundamentals are open and transparent for the implementation mechanisms. Due to speciality of decentralization characteristics ,distribution, anonymity and non- tamperability it can be widely used in various areas such as I0T sector, banking sector, public services and even for the identity management[12][15].

Now by using the core technology of blockchain, we are proposing to re-construct the BGP and make it more secure for the people over the network. When a router announces its prefix origin in a network ,blockchain can help to verify the peer node of the network and verify the hash of the previous node which can help to avoid BGP hijack and DDoS kind of attacks. In order for the routing policy a stack of valid IPs will be stored as a published promise in order to avoid cheat. It also understands easily that which path it should consider for the best connection and session establishment in order to exchange for information[1].

One of the most important component as a crypto primitive for blockchain network which is used for providing users the service of data integrity is hashing functions. Hashing functions are used in various fields other than cryptography as well to provide high quality information security services. Hashing is basically the transformation of an input array of arbitrary length data into a fixed output string. These kind of transformations are called hash functions. Due to the special architecture they are much more efficient in processing the graphical information. This also helps in applying the maximum parallelization of calculation which ultimately results into faster services[13][14].

IV. BGP BLOCKCHAIN

The BGPBlockchain is mainly designed for better and secured BGP over the network and it mainly focuses on the better and improved QoS for the end user by reducing the number of DDoS attacks, data tampering attacks and data falsification attacks.

BGPBlockchain firstly uses the public chain is shown in Figure 2 which will have two kinds of participants: End users and Routers. The use of this public chain over here is that it will store the Router contracts which are generated on original prefixes and it will consume energy on the basis of selection of the most appropriate path for the best data communication over the network.

In the below figure when PC1 establishes session with PC2 , first of all PC1 will look for the best path for session establishment and they pay the energy required for it. When the router accepts this contract the path for the exchange of the communication is scheduled and set. Routers on this path sign the digital certificates of the neighbouring routers. After the transferring of data from PC1 to PC2 the hops which contributed in the establishment of perfect session gets the share of their energy and rest all will not get any energy in BGP network.

The main features of the above model:-

Secured session establishment: A secured session must be uniquely identified and established with the determination of parameters such as the source and destination address and then all the information must be passed in a super secured manner which includes the hashing technique known as BLAKE-256.

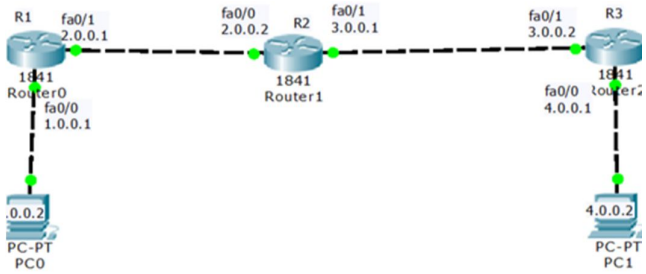

Figure 2. Network architecture

In which PC0 will be at initialization stage and PC1 will be at final stage and all of the information that is passed through the AS moves in a secured way. The source also announces the amount of promised energy for all the hops and now when the data is transferred to Router 0, with the help of blockchain technology it will be made sure that the data going to the destination comes from the authorized autonomous system as there hashes will be checked at all the phases.

All the Routers in BGPBlockchain synchornizes the pending RouteContracts in the AS. On the basis of the routing policies it considers the best RouteContract for the best quality of service for the user in the offered energy. If the end user is of the other AS then the Router tries to establish a connection with the appropriate hop of the best RouteContract and establish the best QoS connection with the other AS with the remained energy.

If a malicious person tries to stop the communication between the source and destination address such as by using a man in a middle attack so the connection will not be made in a pre-defined time and hence the connection will be forcefully re-established.

Data Communication: This process starts once the perfect path is selected in the RouterContract so data is transmitted from the source address to the destination address and the routing quality will be stamped.

V. BGP BLOCKCHAIN MODEL

The sideline technology is used as they have the overlapped participants which will adopt different node and consensus algorithms.

The consensus algorithm is basically divided into two categories of mature blockchain: the Proof of Work (PoW) series and the BFT series. The first one is basically used for the characteristics of weakly trusted nodes in the network and fork problems in public blockchain. While the use BFT series in consortium blockchain for the characteristics of authoritative nodes and high requirement of block consistency. The nodes which come from around the world in QoS based routing in which routers are widely distributed and meanwhile the nodes in resource authentication are authorized entities.

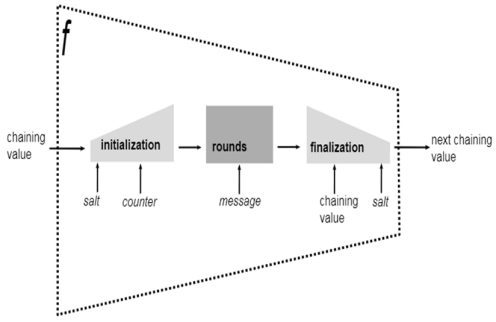

Figure 3. Implementation of Blockchain in BGPBlockchain

The BGPBlockchain consists of both the above mentioned characteristics for the best routing blockchain and the resource authentication of blockchain goes through the three steps

1. First of all the miner is selected randomly from the thousands of miners by calling a voting smart contract in the current system and then after the voting ends the top twenty one miners gets selected randomly from the bunch and gets ready for the block generation phase.
2. Then the second phase starts, where the miners are sorted randomly again and then they uniquely witnesses and collects effective records and collects them into a new block and each miner gets the time of 15s to if the miner doesn't fulfils the requirement by following the consensus algorithm each miner tries to crack the hash and get the node and if in the given time frame the miner completes it's task and does not able to crack the hash then that block is passed to the other miner and the same procedure follows.
3. In the final third stage as per resource authentication adds BFT for the block confirmation so that no security risk could be there. Additionally now no new block requires confirmation and all the miners can follow the existing method of confirmation of block that is after the 1st miner gets the block confirmation the other miner will immediately move to work upon the other node in order to acquire that and in all this after adding the BFT authentication there won't be fault tolerance and will be fully secured.

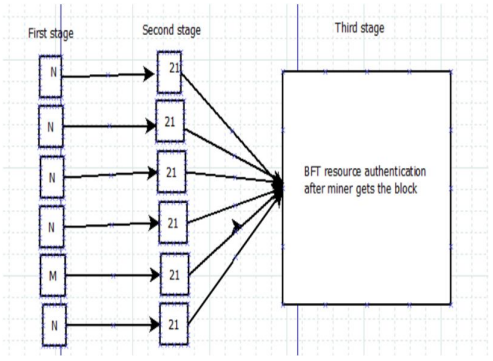

Figure 4. Stages in BGPBlockchain

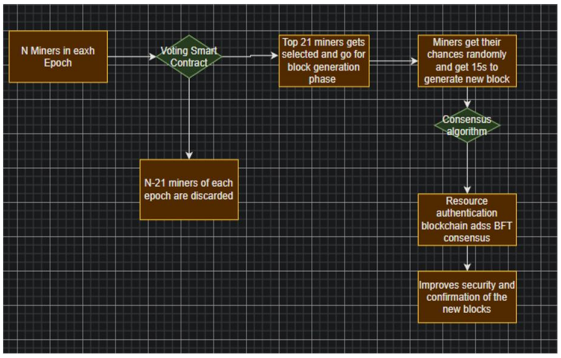

Figure 5. Working of BGPBlockchain

The main goal of all the miners is to acquire the node but not competing and thus if fork occurs, the underlying technology shifts towards the longer side the chain and thus all the other left nodes are authenticated without any fork problem.

VI. Conclusion

BGP protocol is being used all over the internet but still it has a lot of loop holes which includes such as DDoS, man in a middle attack and many more and the challenges related to security of the past protocols and methods of BGP are also increasing and for that a solution is there which can be blockchain which is already getting started to implement in various areas for the enhancement of technology and could be applied for BGP as well to make it more secure from various security threats. Although there is a requirement in order to understand the

implementation part more thoroughly applying consensus algorithm in BGP and a lot of research is required with more hashing techniques.

REFERENCES

[1] Mitseva, A. Panchenko, T. Engel The State of Affairs in BGP Security: A Survey of Attacks and Defenses
[2] Z.Yan1 , G. Geng , H. Nakazato , and Yong-Jin Park Secure and Scalable Deployment of Resource Public Key Infrastructure (RPKI)
[3] M. O. Nicholes, B. Mukherjee, A Survey of Security Technologies for the Border Gateway Protocol (BGP), IEEE Communications Surveys & Tutorials 11 (1) (2009) 52–65.
[4] T. Wan, P. C. van Oorschot, E. Kranakis A Selective Introduction to Border Gateway Protocol (BGP) Security Issues, in: NATO Advanced Studies Institute on Network Security and Intrusion Detection, IOS Press, 2005.
[5] K. Butler, T. R. Farley, P. McDaniel, J. Rexford A Survey of BGP Security Issues and Solutions, Proceedings of the IEEE 98 (1) (2010) 100–122.
[6] Al-Musawi, P. Branch, G. Armitage BGP Anomaly Detection Techniques: A Survey, IEEE Communications Surveys & Tutorials 19 (1) (2016) 377–396.
[7] Blockchain based Inter-domain Latency Aware Routing Proposal in Software Defined Network
[8] Satoshi N., Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System Bitcoin (2008)
[9] 10 J. -H. Lee BIDaaS: Blockchain Based ID As a Service
[10] B. Bhushan, P. Sinha , AndrewJ Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions
[11] 12 Salman T., Zolanvari M., Erbad A., Jain R., Samaka M.
[12] S Shukla, M Kumar, An improved energy efficient quality of service routing for border gateway protocol, Computers & Electrical Engineering, Volume67,2018, Pages520-535 Security services using blockchains: A state of the art survey IEEE Commun. Survev. Tutor., 21 (1) (2019), pp. 858-880
[13] I. Eyal, A. E. Gencer, E. G. Sirer and R. V. Renesse, "Bitcoin-NG: A scalable blockchain protocol", Proc. 13th Usenix Conf. Netw. Syst. Design Implement. (NSDI), pp. 45-59, 2016
[14] S Shukla, M Kumar An improved quality path selection approach for border gateway protocol Int J Intell Eng Syst, 10 (5) (October 2017), pp. 11-18
[15] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things", IEEE Access, vol. 4, pp. 2292-2303, 2016.
[16] 1 T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security Services Using Blockchains: A State of the Art Survey," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 858-880, Firstquarter 2019, doi: 10.1109/COMST.2018.2863956 https://ieeexplore.ieee.org/abstract/document/8428402
[17] S Shukla, M Kumar Improving convergence in iBGP route reflectors, Lecture Notes in Electrical Engineering, 443 (October 2017), pp. 381-388