Blockchain-based strategy for securing BGP routing and the design of the smart contract

Graciela Becci[1] , Miguel Morandi[1] , Marcelo Gómez[1]

[1] Universidad Nacional de San Juan, Argentina
{gbecci, morandi, mgomez)@unsj.edu.ar

Abstract. BGP Border Gateway Protocol is the Internet routing protocol, responsible for the connectivity in the Internet. BGP guarantees Internet connectivity between Autonomous Systems AS in a decentralised manner. Since its origins, BGP has been based on mutual trust between ASes, particularly with regard to route advertisements. However, in practice there have been cases in which route advertisements have been blocked or diverted to a non-intended destination, due to either operator's inexperience or intentionality, giving rise to Internet disruptions in the form of denial of service, or route hijacking. Alternative solutions have been developed by official organisations, leaders of the sector and researchers. However, none of these solutions has been widely accepted. Blockchain as a distributed ledger, offers a decentralised, peer-to-peer, and generally incorruptible chain of blocks of records linked together by cryptographic hashes, guaranteeing the immutability of each transaction. In this article, these blockchain characteristics are tha base for the design of a BGP security strategy, which include as the main actors the RIR and the ASes owners. This solution helps the border router operators to retrieve information to build informed routing decisions for securing BGP routing protocol.

Keywords: external BGP routing, routing security, blockchain.

1. Introduction

BGP Border Gateway routing Protocol is the Internet routing protocol, responsible for the connectivity in the Internet. Like a road-map, BGP provides the most efficient way to reach a destination, assuring the reachability, while avoiding loops and latency. BGP guarantees Internet connectivity between Autonomous Systems AS in a decentralised manner. Since its origins, BGP has been based on mutual trust between ASes, particularly with regard to route advertisements. However, in practice there have been cases in which route announcements have been blocked or diverted either by operator inexperience or intentionally, giving rise to Internet disruptions in the form of denial of service, or route hijacking.

Alternative solutions have been developed by official organisations, leaders of the sector and researches, such as BGP protocol extensions from IETF, solutions applying

symmetric and asymmetric cryptography, and even proposing overlay networks. However, none of these solutions has been widely accepted. Blockchain as a distributed ledger, offers a peer-to-peer, decentralised, generally incorruptible chain of blocks or records linked together by cryptographic hashes. Blockchain, as a disruptive technology, offers security in the registration of valuable information, guaranteeing the immutability of each transaction by its digital signature. Blockchain structure is similar to BGP external routing as it is composed of geographically distributed ASes. Considering that BGP security is still a relevant topic for the connectivity on the Internet, blockchain offers an alternative technology to guarantee security, transparency, and decentralised access to routing information. The objective of the proposed project is to improve the security in external BGP, with the aim of developing a model of smart contract applicable to security solutions in Blockchain.

This project has two main objectives, firstly to analyse BGP security requirements and existing solutions, and secondly to develop a smart contract model to be tested with a generic use case. This article is organised as follows: Section 2, Background of BGP Security Solutions, Section 3, blockchain-based strategy design, Section 4, Smart Contract deployment, and Section 5. Conclusions and Future work.

2. Background of BGP Security Solutions

2.1 BGP Best Practices

BGP best practices are widely adopted techniques to avoid common security problems [1]. This type of solution recommends route and AS-path filtering between Internet Service Provider ISP and customers, and between peers [2]. It is also recommended to filter out special-use IP addresses, announcements containing private ASN, and too long AS-paths. The restriction of advertisements of networks smaller than /24 prevents the size explosion of routing tables.

2.2 Securing Control Plane

Threats in the Control Plane relate to routing information and route announcements, mainly to the UPDATE message: IP prefix validation, AS-path origin validation and authorisation, and routing policies [3].

DNS-based proposals have the objective of validating the IP prefix delegation and path origin authentication. A new DNS zone administered by IANA has been proposed as a distributed database for origin validation [4]. On the arrival of an UPDATE message, BGP routers can verify the consistency between the NLRI of the received IP prefix and the information in the DNS structure. However, the creation of a new DNS hierarchy introduces considerable overhead in the system management.

Proposals relying on overlay networks suggest the use of complementary protocols such as Inter-domain Routing Validation protocol IRV, and the implementation of a SDN-based IXP [5]. The separation of the control and data plane allows for more complex routing policies and filtering, albeit the overhead in the network setup. These proposals do not modify the BGP protocol and do not require router reconfiguration. However, they tend to slow down routing convergence when routing changes emerge in overlay networks.

2.3 Securing Data Plane

Attacks in the data plane relate to packets misrouted (dropped, rerouted or delayed) by intermediate ASes [3]. One way of detecting anomalies in the data plane is by verifying the consistency between announcements and actual forwarding routes.

Traceroute as a diagnostic tool does not scale in the Internet, and the routing information is not directly derived. An AS-level traceroute tool has been proposed taking information from initial BGP routing tables at different geographic points [6]. However, this information is not always updated nor disclosed.

A proposal using encrypted tunnels between routers does guarantee the end-to-end connectivity, but the full path integrity can be compromised to misrouting the traffic [7]. Encrypted solutions require off-line exchange of keys and collaboration between ASes, thus these types of solutions do not scale well.

The digital signature included in the announcement message is intended for origin authorisation. This method requires a modification of the BGP UPDATE message, and the lack of encryption opens a vulnerability to tamper the routing data [3].

2.4 Encryption to secure BGP

While symmetric keys encryption uses the same key to encrypt and decrypt the message, asymmetric keys encryption requires a pair of public and private keys. Symmetric encryption provides only confidentiality, while asymmetric encryption provides confidentiality, authenticity and non-repudiation.

Proposals relying on Symmetric Cryptography

When securing BGP, symmetric cryptography allows for faster signing procedure, though the protocol overhead increases with the authentication process. Proposals such as Message Authentication Code MAC and Source Path Vector allow for AS-Path validation [8]. The MAC proposes a nested authentication code to be included in the UPDATE message, which contains the authentication key of each AS in the path. The validator node recursively verifies the authenticity of the AS path information. Source Path Vector uses trees of classifying hash chains to detect path modification. However, symmetric keys are vulnerable to brute force attacks.

Proposals relying on Asymmetric Cryptography

Secure-BGP S-BGP uses digital signature and public key certificates to validate routing data [9] verified by a PKI Public Key Infrastructure. S-BGP includes Address Attestation AA, which is a digitally signed certificate by the resource holder, consisting of the ASN and the assigned IP prefixes, stating that an AS has the right to originate a route to an IP prefix. The AA is distributed out-of-band and verified through the certificate chain to IANA. AA prevents IP prefix hijacking but does not prevent modification of the AS path. S-BGP covers most of the BGP security threats but requires a considerable management load, leading to a slow adoption.

Secure Origin BGP soBGP was designed to improve S-BGP performance [8]. SoBGP is based on three types of certificates: ASN certificate issued by a trusted authority, certificate that binds ASN to a set of IP prefixes, and a certificate of routing policies and neighbour ASes of each AS. These certificates help each router to build a

network topology. When an UPDATE message arrives, the AS path is compared to the topology, in case of mismatch the route is dropped. The router topology is rather static and it does not follow fast network changes lowering the network performance.

Pretty secure BGP psBGP implements ORIGIN authorisation by building a distributed trust model between ASes to validate AS path of the announcements [10]. Unlike IP prefixes, the AS numbers can be managed by a PKI due to the limited number compared to IP prefixes. Therefore this strategy uses a certificate hierarchy where each AS has to rate neighbour ASes to create an IP prefix assertion list containing its own and neighbours' rating of address ownership. When an UPDATE message arrives, the path origin is validated according to the reputation from ASes in the assertion list. The lack of adoption of psBGP is explained by the "weak form of origin authentication" [10] because the ASes have to rate unknown information from other ASes, and also because the BGP UPDATE message requires a modification.

IETF proposals

RPKI. IETF Secure Inter-Domain Routing Working Group SIDR WG presented the standardised architecture RPKI Resource Public Key Infrastructure to provide a global origin authorisation [11]. The Route Origin Authorisation ROA certificate authorises an AS to advertise determined IP prefixes and the maximum length.

BGPsec. SIDR WG developed the BGPsec as an extension to BGP. BGPsec carries digital signatures in the non-transitive AS Path attribute propagated in the UPDATE message [8]. This signed message assures that the paths in the AS Path list are responsible for the particular IP prefix propagation and authorise the propagation of the UPDATE message. In the end, the AS Path is included in the UPDATE message and in the sequence of ASes involved in the propagation of the IP prefix. BGPsec cannot be deployed gradually and when a non-BGPsec speaker is included in the AS path the BGPsec information is not available, breaking the security chain. To summarise BGP security approaches, Mitseva et al. present four categories of solutions according to the degree of protection [3]:

1. **OA**. Origin authorisation and the ROA certificate of ASN and IP prefix allocation
2. OA+1. Origin authorisation, adjacent neighbour ASes, and the AS path-end
3. **RTPV**. Routing Topology Path Verification, such as soBGP that builds a topology of ASes connectivity
4. **PV** Path Validation, solutions such as S-BGP, psBGP, and BGPsec, validates also the ASes included in the route to the IP prefix.

2.5 Blockchain-based BGP Security Solutions

Blockchain is one form of distributed ledger technology DLT, designed to administer an online and immutable record of verified data and transactions [12]. The DLT is based on a peer-to-peer network, which uses a consensus algorithm to agree on transactions, to be replicated in every node of the chain [13].

Each transaction and the related data is verified and recorded in an individual block, which is permanently linked to a previous similar record [14]. The hash of the data is then stored in the distributed nodes of the blockchain, if a node fails the chain still exists, adding robustness to single-point-of-failure. As a one-way encryption system, the hash cannot be decrypted to make the data readable again, contributing to

the confidentiality of the information [15]. The hash as a cryptographic digest of the data, helps also to reduce the storage space.

Blockchain may function as an alternative to third party data verification infrastructure [16]. Instead of a central authority certifying data, blockchain can be used as a distributed authenticating and auditing system, due to the proof of ownership and timestamp of each transaction. Therefore, blockchain technology has important features to add value to the security in the inter-domain routing [17]. The following are proposals of solutions in the research literature.

BGPcoin proposes a repository infrastructure for resources assignment and attestation, providing Route Origin Authorisation ROA, and the attestation of neighbourhood ASes at the last hop denominated AS-Path-end [18].

Ipchain is designed as a management of resources, for storage, allocation and delegation of IP addresses, providing ROA certification [19].

A **blockchain-based validator** system is designed for storage and validation of transactions: assignment and revocation of IP-Prefix to ASes (ROA), and announcement and withdrawal of AS-Path and AS-Path-end verification [20].

RouteChain is a blockchain-based BGP routing system, with a bi-hierarchical structure to validate ROA, AS-Path and AS-Path-end [21]. The bi-hierarchy is intended to reach faster consensus, and is composed by a global chain of subgroups, and several subgroups of chains of the geo-distributed ASes.

BRVM Blockchain-based Routing Verification Model verifies the AS-Path policy particularly whether a route violates the shortest path policy [22].

Drawbacks of blockchain-based solutions

The drawback of blockchain to support BGP routing is mainly due to the scalability factor and the time to reach consensus [17]. Scalability issues are due to the large number of ASes and routing transactions, hindering the blockchain consensus, while the blockchain real-time update to the routers slows down network convergence [18].

Trade-off between loads of incoming transactions poses a risk to blockchain robustness [20]. Larger loads require more transactions within a block and faster mining time to reach consensus, and it is easier for attackers to reach faster mining time as a proof-of-work to get power to corrupt the chain. The trade-off between throughput and storage limits the information to be stored in the blockchain [19].

Consensus mechanisms may lead to a monopoly [19], for instance the Proof-of-Stake PoS consensus algorithm, where powerful nodes may control the entire blockchain by controlling the majority of assets [18]. All these strengths and weaknesses are opportunities to develop new efficient solutions. The next section describes the strategy design for securing BGP routing using blockchain.

3. Blockchain-based Strategy Design

3.1 Strategy for securing BGP routing

The strategy for securing BGP routing followed in this work focuses on the development of a smart contract for route-origin authentication and path validation.

Based on BGP vulnerabilities and solutions reviewed in Section 2, it has been concluded that the validation of AS-path is crucial in securing BGP. The seminal works in which this project is based are described in the following paragraphs.

Blockchain-based solutions range from reproduction of a RPKI system in a blockchain, to ROA certification and path validation. However, there is no evidence of widespread development, and only a few examples are well documented.

To secure the interdomain routing, Cohen et al. propose a complement to RPKI method that validates the last-hop of the AS path, denominated path-end validation [23]. The n-1 AS path is also validated to guarantee that the n-1 AS holds the ownership of the published prefixes.

Unlike BGPsec, which requires the cryptographic validation of every single hop in the AS path, and the upgrading of the routing hardware, path-end validation method allows for a partial validation, without the need of hardware changes [8].

In this way, it is difficult for an attacker to be situated in the neighbourhood of the target AS, due to business relations among ASes, forcing the attacker to fake a path greater than one hop, resulting in a longer AS path, with lower likelihood of becoming a preferred path. This approach is appropriate for implementing in a blockchain, as it does not rely on a centralised RPKI structure, and has been proved that a partial deployment has better adoptability.

Mastilak et al. propose a blockchain-based RPKI hierarchical structure [24]. In this work IANA uses a BGP Management system in blockchain to administer the RIR, LIR, and ISPs. These registries use blockchain to allocate and revocate prefixes, and issue ROA certificates, which can be later used by border routers to validate the routes. This solution, like RPKI, requires the adoption by all members of the structure to secure the handshaking of information between the hierarchy levels. BGPcoin [18] and McaBranches project [25], focuses on the route-origin authentication in blockchain. The following section describes the design of the selected strategy.

3.2 Smart Contract design methodology

The strategy in this project for securing BGP routing aims at validating the route origin and the AS path. Thus, the design of the related smart contract contains three main functionalities: routing certificate generation, sign and verification, and BGP advertisement and validation as a service.

The smart contract has been developed, compiled and deployed in the Ethereum platform Remix using solidity language. The analysis of the solution has been documented by use cases and sequence diagrams, to describe the main requirements, actors, actions, requests and results of the whole process. The following paragraphs describe the functionalities and the related sequence diagrams.

Functionality 1: Blockchain Resources Registration and Certificates Generation

Precondition. The registration in the blockchain requires firstly that the AS Owner request authorisation to the RIR to start transactions in the blockchain.

1. AS Owner Registration

1.1 AS Owner request to the RIR authorisation to operate in the blockchain.

1.2. The RIR validates the AS Owner against the RPKI resource registry, and issues a certified smart contract SC identified with a unique address, which allows the AS Owner to perform blockchain transactions.

1.3. The AS Owner/Admin's first transaction is to add to the blockchain the AS Owner identified by the Owner Public Key:
SC function: *add_Owner (PublicKeyOwner)*
2. ASN Registration
2.1. The AS Owner registers in the blockchain the AS Numbers linked to the Owner.
SC function: *add_ASN (ASN, PublicKeyOwner)*
3. Prefix Registration
3.1. The AS Owner registers in the blockchain the assigned prefixes, linked to ASN by using the procedure Sign & Verification.
SC function: *add_Prefix (ASN, Prefix, Mask, ...)*
The Sequence Diagram in Fig. 1 shows the main transactions to the blockchain for Resource Registration and Certificate Generation.

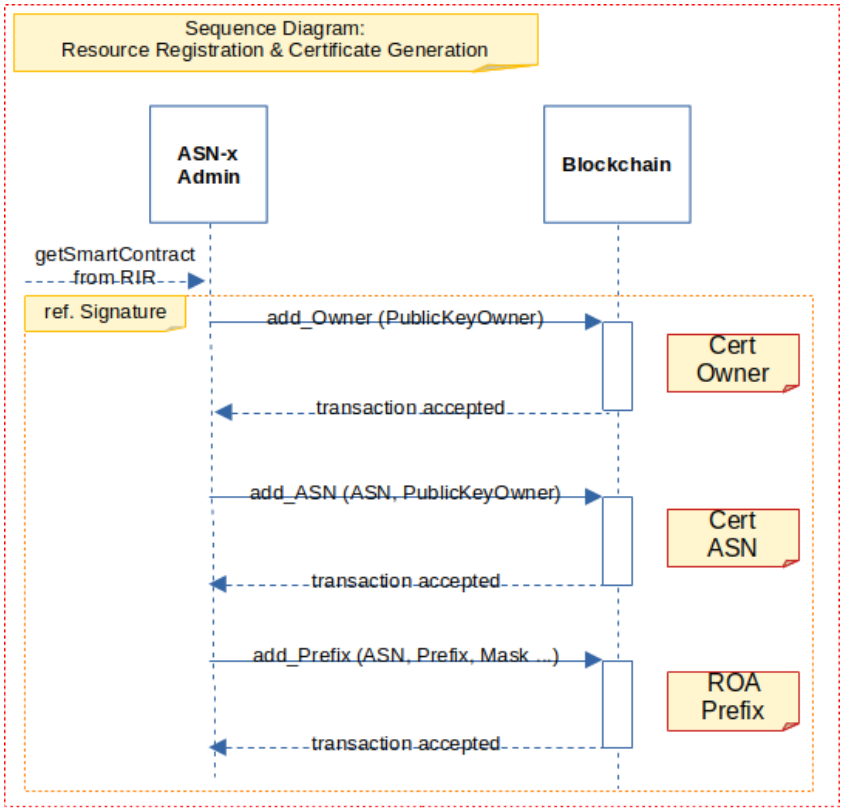


Figure 1. Sequence Diagram for Resource Registration and Certificate Generation. The AS Owner gets a certified smart contract from the RIR. This allows the AS Admin to register the AS Owner, AS Number and AS Prefixes in the blockchain.

Functionality 2: Signature and Verification of the blockchain transactions
Message Signature ON-CHAIN shown in Fig. 2
1. AS Admin gets the message hash, which includes ASN and Prefixes.
SC function: *get_Message_Hash(ASN, Prefix, Mask)*

2. AS Admin signs message using Keccak-256, the Ethereum hashing algorithm.
SC function: *get_Ethereum-sigend(MessageHash)*
Signature Verification OFF-CHAIN shown in Fig. 2
1. AS Admin signs the message hash using a crypto wallet like MetaMask.
SC function: *sign_MetaMask_Message(ASN, Prefix)*
2. Signatures produced by Keccak-256 and Metamask must be the same.

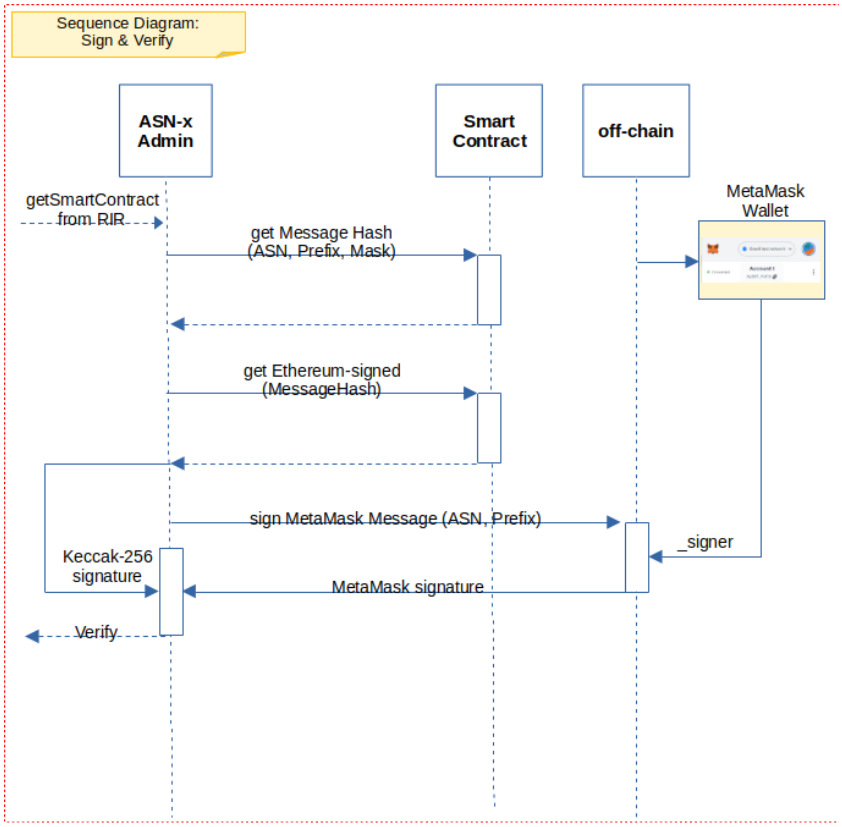


Figure 2. Sequence Diagram for Signature and Verification. Blockchain transaction messages are hashed and signed using keccak-256, while the verification procedure is done off-chain by calculating the message hash using a crypto wallet like MetaMask.

Functionality 3: BGP Advertisement and Validation as a service
1. AS's border router Admin advertises its own routes and the transaction is stored in the blockchain, shown in Fig. 3: SC function: *add_Advertisement(ASN, Prefix, Mask, NextHop)*
2. AS Admin validates in the blockchain the authenticity of incoming advertisements done by other ASes: SC function: *validAdvert()*
3. AS Admin validates the Owner of received Prefixes:
SC function: *getPrefixOwner(Prefix, Mask)*
4. AS Admin can request a Prefix list by ASN: SC function: *getPrefixByASN(ASN)*

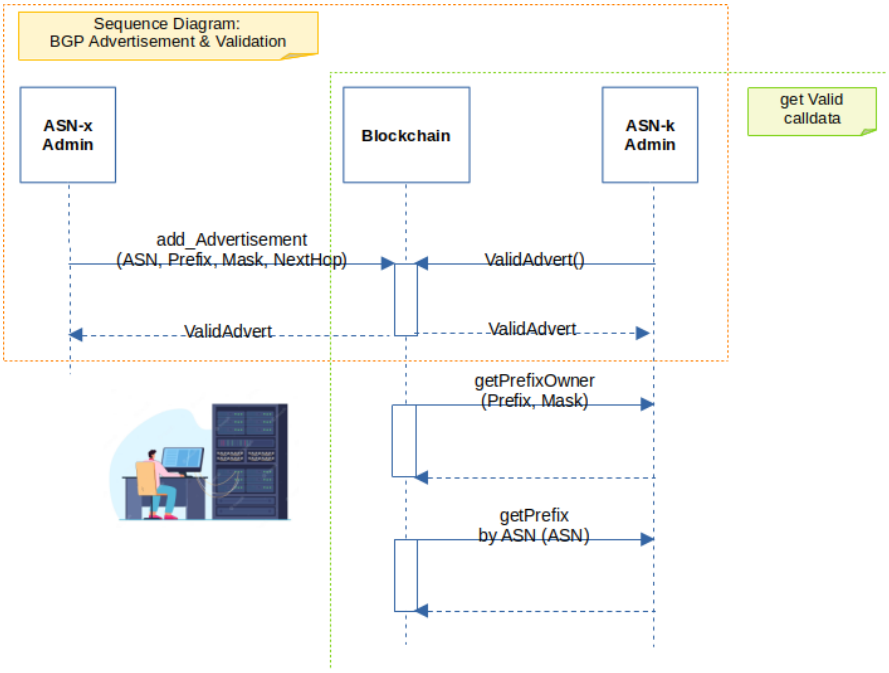
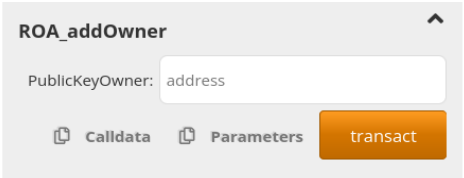


Figure 3. Sequence Diagram for BGP Advertisement and Validation. The BGP advertisement by a particular AS stored in the blockchain can be validated by any other network admin, provided their ASN is registered in the blockchain. The validation can include, advertisement validation, get the owner of a prefix, and get prefixes by ASN.

4. Smart Contract Deployment

Related to the smart contract design and deployment the following tables summarise the strategy for securing BGP, describing the three functionalities. Table 1 a) shows Functionality 1, Blockchain Resources Registration and Certificates Generation, particularly the case of adding AS Owner and AS Number.

Table 1 a). Blockchain Resources Registration. Blockchain transactions to add the AS owner, and AS Number. The AS owner is associated with the smart contract address.



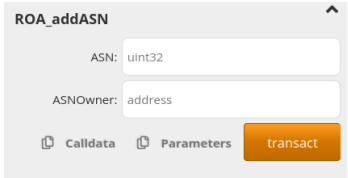
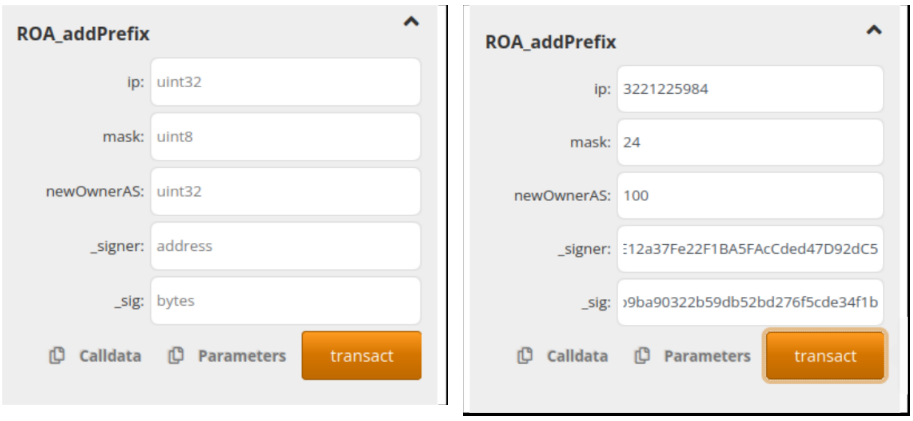


Table 1 b) shows the add Prefix function, the certificate contains information about the IP address, mask and AS number. This information is hashed and signed off-chain

using the MetaMask account address (_signer), and resulting in a hashed certificate (_sig), stored in the blockchain. The example refers to the prefix as the decimal expression of the IP address for documentation, which is 192.0.2.0/24.

Table 1 b). Blockchain Resources Registration - add Prefix. The certificate stored in the blockchain contains information about the IP address, mask and AS number. The MetaMask address (_signer) for signing the message, and the hashed certificate (_sig).



Functionality 2. For Signature and Verification of the blockchain transactions firstly, the message (prefix and AS number) is hashed, and secondly, the hashed message is signed. The results in an Ethereum signed message are shown in Tables 2 a) and b).

Table 2 a). Signature and Verification. Hash the data to be signed: IP, mask and ASN

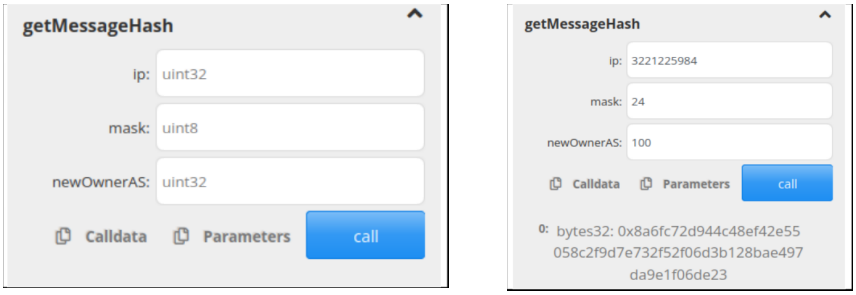
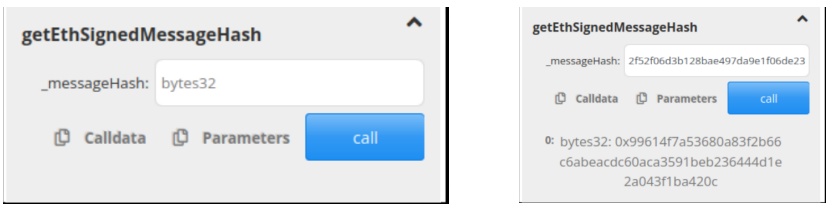
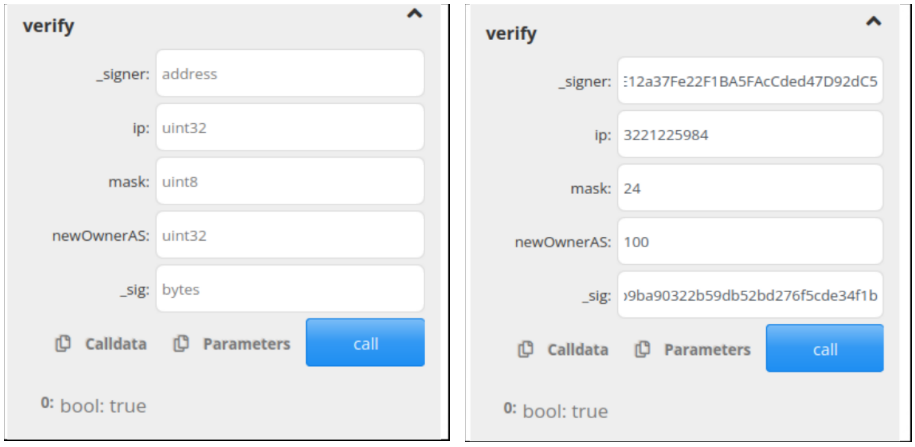


Table 2 b). Signature and Verification. Sign the hashed information using Keccak-256



The signature verification compares the recovered ethereum signed message with the MetaMask address returning a boolean value. The certificate parameters (prefix and AS number) are passed to the function verify, together with the MetaMask address (_signer) and the signed certificate (_sig). Table 2 c) shows the case of matching addresses giving a boolean “TRUE” result.

Table 2 c). Signature and Verification. Verifying the signature implies comparing the recovered Ethereum signed message with the MetaMask address, returning a boolean result “TRUE” in this case.



Functionality 3. BGP Advertisement and Validation as a service.
Table 3 a) shows BGP Advertisement and Validation - get verified calldata, as an on-chain service, requesting information of the prefix owner and prefixes listed by ASN.

Table 3 a). BGP Advertisement and Validation. The function getPrefixOwner() retrieves the AS owner of a given prefix, and getPrefixByAS() retrieves all prefixes assigned to an AS.

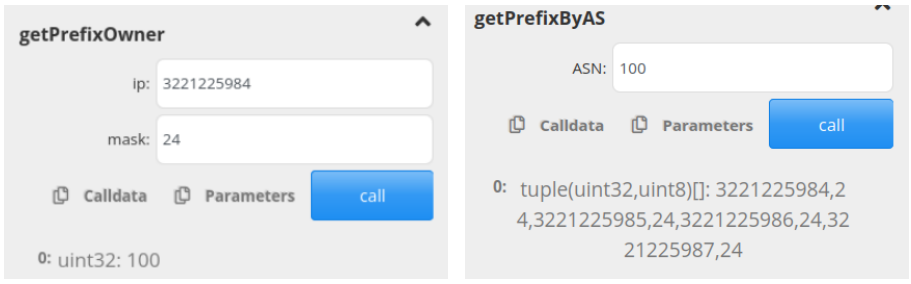
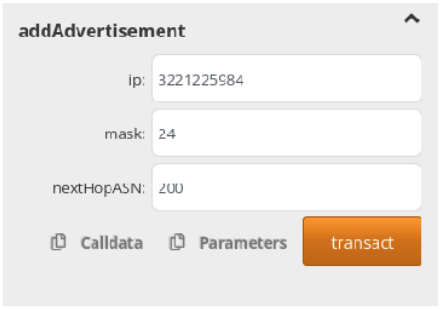
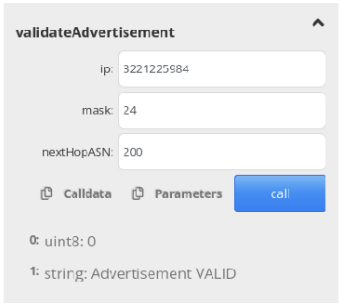


Table 3 b) shows the BGP Advertisement and validation functionality, prefix and next-hop information. This information stored in the blockchain allows any AS registered in the system to query the network to validate the received advertisement.

Table 3 b). BGP Advertisement and Validation. The function addAdvertisement() stores in the blockchain the prefix and the next-hop AS Number, while the function validate Advertisement() retrieves a boolean result of a calldata to a prefix and next-hop ASN.





The smart contract deployment for securing BGP external routing has been done using an Ethereum Virtual Machine in Remix, to gain experience while disregarding deployment constraints. This also allowed for a better understanding of the implementation of solidity structures and gas consumption.

5. Conclusions and Future work

The proposed blockchain-based strategy for securing BGP external routing includes three functionalities: Blockchain Resources Registration and Certificates Generation, Signature and Verification of blockchain transactions, and BGP Advertisement and Validation. This allows the AS Owner to register the AS resources, and routing advertisements, while any AS Admin can get certificates and validated routing information from the ASes' community. The routing information stored in the blockchain intends to add security to BGP routing, in addition to becoming transparent and auditable transactions, as inherent characteristics of blockchain.

The contribution of this project is the proposed blockchain-based strategy for securing BGP external routing and the development of the related smart contract, as a resource that can be managed by a RIR to improve the security of Internet routing, additionally to existing routing validators and securing methods and protocols.

In this design stage there are no considerations about gas consumption nor blockchain performance. The deployment in a test-net and performance evaluation are left for future work.

References

[1] NSA National Security Agency, “NSA Cybersecurity: A Guide to Border Gateway Protocol (BGP) Best Practices,” NSA Cybersecurity publications. Accessed: Apr. 11, 2024. [Online]. Available: https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-guide-to-border-gateway-protocol-best-practices.pdf

[2] J. Snijders, “Practical everyday BGP filtering with AS_PATH filters: Peer Locking,” presented at the NANOG-67, Chicago, Il: NANOG North American Network Operators Group, Jun. 2016. [Online]. Available: https://archive.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf

[3] A. Mitseva, A. Panchenko, and T. Engel, “The State of Affairs in BGP Security: A Survey of Attacks and Defenses,” Computer Communications, vol. 124, Apr. 2018, doi: 10.1016/j.comcom.2018.04.013.

[4] J. A. Hawkinson and T. J. Bates, “Guidelines for creation, selection, and registration of an Autonomous System (AS),” Internet Engineering Task Force, Request for Comments RFC 1930, Mar. 1996. doi: 10.17487/RFC1930.

[5] X. Zhao, S. S. Band, S. Elnaffar, M. Sookhak, A. Mosavi, and E. Salwana, “The Implementation of Border Gateway Protocol Using Software-Defined Networks: A Systematic Literature Review,” IEEE Access, vol. PP, pp. 1–1, Aug. 2021, doi: 10.1109/ACCESS.2021.3103241.

[6] Z. M. Mao, J. L. Rexford, J. Wang, and R. H. Katz, “Towards an Accurate AS-Level Traceroute Tool,” in Computer Communication Review, Association for Computing Machinery (ACM), Oct. 2003, pp. 365–378. doi: 10.1145/863993.863996.

[7] I. Avramopoulos and J. Rexford, “Stealth Probing: Efficient Data-Plane Security for IP Routing.,” Jan. 2006, pp. 267–272.

[8] G. Huston, Geoff, “A Survey on Securing Inter-Domain Routing Part 2 – Approaches to Securing BGP | blabs.” Accessed: Apr. 11, 2024. [Online]. Available: https://labs.apnic.net/index.php/2021/08/03/a-survey-on-securing-inter-domain-routing-part-2-approaches-to-securing-bgp/

[9] S. Kent and A. Chi, “Threat Model for BGP Path Security,” Internet Engineering Task Force, Request for Comments RFC 7132, Feb. 2014. doi: 10.17487/RFC7132.

[10] K. Butler, T. Farley, P. McDaniel, and J. Rexford, “A Survey of BGP Security Issues and Solutions,” Proceedings of the IEEE, vol. 98, pp. 100–122, Feb. 2010, doi: 10.1109/JPROC.2009.2034031.

[11] R. Bush and R. Austein, “The Resource Public Key Infrastructure (RPKI) to Router Protocol,” Internet Engineering Task Force, Request for Comments RFC 6810, Jan. 2013. doi: 10.17487/RFC6810.

[12] S. Ray, “The Difference Between Blockchains & Distributed Ledger Technology,” Medium. Accessed: Apr. 11, 2024. [Online]. Available: https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92

[13] R. Maull, P. Godsiff, C. Mulligan, A. Brown, and B. Kewell, “Distributed ledger technology: Applications and implications,” Strategic Change, vol. 26, pp. 481–489, Sep. 2017, doi: 10.1002/jsc.2148.

[14] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, “Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems,” IEEE Consumer Electron. Mag., vol. 7, no. 4, pp. 6–14, Jul. 2018, doi: 10.1109/MCE.2018.2816299.

[15] J. Katz and Y. Lindell, “Introduction to Modern Cryptography,” Routledge & CRC Press. Accessed: Apr. 11, 2024. [Online]. Available: https://www.routledge.com/Introduction-to-Modern-Cryptography/Katz-Lindell/p/book/9780815354369

[16] G. He, W. Su, S. Gao, and J. Yue, “Securing Route Origin Authorization with Blockchain for Inter-Domain Routing,” 2020 IFIP Networking Conference (Networking), Jun. 2020, Accessed: Apr. 11, 2024. [Online]. Available: https://www.semanticscholar.org/paper/Securing-Route-Origin-Authorization-with-Blockchain-He-Su/a6d7720cc650ede3db61047167b3bc59b829b5b1

[17] L. Mastilak, P. Helebrandt, M. Galinski, and I. Kotuliak, “Secure Inter-Domain Routing Based on Blockchain: A Comprehensive Survey,” Sensors, vol. 22, no. 4, Art. no. 4, Jan. 2022, doi: 10.3390/s22041437.

[18] Q. Xing, B. Wang, and X. Wang, “BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution,” Symmetry, vol. 10, no. 9, Art. no. 9, Sep. 2018, doi: 10.3390/sym10090408.

[19] J. Paillisse, J. Manrique, G. Bonet, A. Rodriguez-Natal, F. Maino, and A. Cabellos, “Decentralized Trust in the Inter-Domain Routing Infrastructure,” IEEE Access, vol. 7, pp. 166896–166905, Jan. 2019, doi: 10.1109/ACCESS.2019.2954096.

[20] I. Sfirakis and V. Kotronis, “Validating IP Prefixes and AS-Paths with Blockchains,” ArXiv, Jun. 2019, Accessed: Apr. 11, 2024. [Online]. Available: https://www.semanticscholar.org/paper/Validating-IP-Prefixes-and-AS-Paths-with-Sfirakis-Kotronis/e7fc32c8f0c5e6f0678df26a2f525cced0e28bf2

[21] M. Saad, A. Anwar, A. Ahmad, H. Alasmary, M. Yuksel, and A. Mohaisen, “RouteChain: Towards Blockchain-based Secure and Efficient BGP Routing,” in 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), May 2019, pp. 210–218. doi: 10.1109/BLOC.2019.8751229.

[22] Y. Liu et al., “A novel routing verification approach based on blockchain for inter-domain routing in smart metropolitan area networks,” Journal of Parallel and Distributed Computing, vol. 142, Apr. 2020, doi: 10.1016/j.jpdc.2020.04.005.

[23] A. Cohen, Y. Gilad, A. Herzberg, and M. Schapira, “Jumpstarting BGP Security with Path-End Validation | Proceedings of the 2016 ACM SIGCOMM Conference.” Accessed: Apr. 11, 2024. [Online]. Available: https://dl.acm.org/doi/10.1145/2934872.2934883

[24] L. Mastilak, M. Galinski, P. Helebrandt, I. Kotuliak, and M. Ries, “Enhancing Border Gateway Protocol Security Using Public Blockchain,” Sensors (Basel), vol. 20, no. 16, p. 4482, Aug. 2020, doi: 10.3390/s20164482.

[25] Mcabranches, “mcabranches/bgp_ethereum.” Jan. 25, 2020. Accessed: Apr. 11, 2024. [Online]. Available: https://github.com/mcabranches/bgp_ethereum