Workgroup: Network Working Group
Internet-Draft:
draft-mcbride-rtgwg-bgp-blockchain-01
Published: 29 June 2022
Intended Status: Informational
Expires: 31 December 2022
Authors: M. McBride D. Trossen D. Guzman
Futurewei Huawei Huawei

BGP Blockchain

Abstract

A variety of mechanisms have been developed and deployed over the years to secure BGP including the more recent RPKI/ROA mechanisms. Is it also possible to use a distributed ledger such as Blockchain to secure BGP? BGP provides decentralized connectivity across the Internet. Blockchain provides decentralized secure transactions in a append-only, tamper-resistant ledger. This document reviews possible opportunities of using Blockchain to secure BGP policies within a domain and across the global Internet.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 31 December 2022.

Copyright Notice

document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

There have been many proposed solutions to help secure the Border Gateway Protocol (BGP) [RFC4271] including securing TCP, CoPP, IPSec, Secure BGP, Route Origination Validation (ROV), BGPSec along with many variations. Could we also use Distributed Consensus Systems (DCS) such as Blockchain to secure BGP? This document provides a review of how such DCSs could be used to secure BGP particularly as supplements to existing solutions. Many of the proposals can be extended to any routing protocol but the focus here is with BGP. The potential attractiveness of adding DCS capabilities to BGP is that it adds additional security without changes to the BGP protocol. Blockchain for BGP proposals are out of band to BGP, similar to RPKI, and not suggesting new encodings. This analysis does not consider external factors such as the energy demands of deploying such solutions.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. A Strawman for a simple BGP Distributed Consensus System

Smart contracts are programs (state machines), executed within a DCS, that run when predetermined conditions are met. These contracts are executed automatically without an intermediary's involvement. Smart contracts may be used in financial, real estate, etc environments to automatically trigger predefined agreements between parties. A DCS implements a smart contract in the form of a distributed state machine, i.e., actions over a pool of information, where distributed DCS nodes maintain the evolving state information over time, utilizing proof techniques, such as proof-of-work, proof-of-stake, and others, to ensure consensus over the latest valid information pool (and thereby the latest state of the smart contract). In popular Blockchain systems, this information pool is represented by the longest blockchain that can be retrieved from the system by a client, i.e., representing the current consensus among the DCS nodes being queried by the client.

With this in mind, we can now describe a simple BGP DCS as one consisting of N miners, which implement the distributed consensus for a desired smart contract, utilizing a suitable proof technique for the consensus. A DCS may implement more than one smart contract, representing, e.g., different BGP capabilities as outlined later in Section 3.

In addition, there are M clients inserting transactions into the system. Those transactions relate to the desired smart contract or may be retrievals of the latest valid consensus information.

Clients and miners may be different entities or they may the same, whereby in the latter case M=N.

The figure below outlines a simple BGP DCS architecture, with BGPs providing clients to the DCS system.

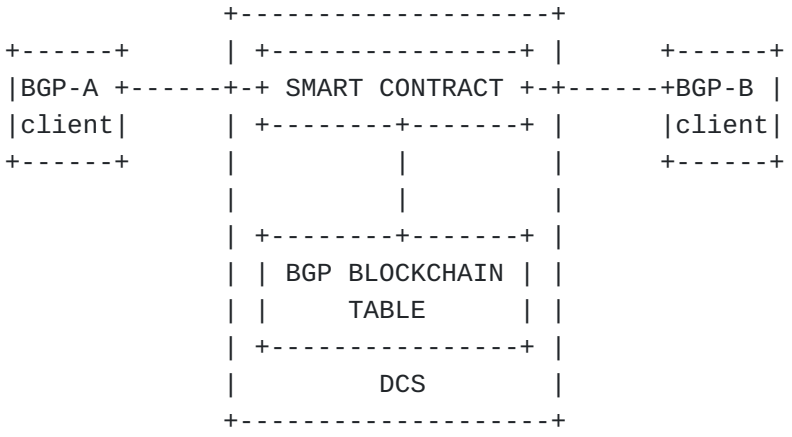

Figure 1: BGP DCS Architecture

In our context of BGP, we can see actions over BGP information, such as BGP origins, routing policies or others, as smart contracts over which distributed consensus needs to be achieved; Section 3 elaborates on those examples. Through using such smart contracts (over BGP information), a DCS for BGP would avoiding BGP human configuration errors or hijacks as common threats for BGP, instead storing transaction information in the DCS where the consensus here represents the latest valid BGP information.

In terms of trust assumptions, a DCS for BGP may require authentication to prevent fraudulent DCS transactions, such as fraudulent BGP announcements being made. For this, the existing RPKI system could be used to authorize any client before sending suitable smart contract transactions into the DCS. If not using RPKI, the DCS would need to check a separate IRR prefix/AS database, if one were to exist, in order to validate incoming transactions on the main DCS before executing them; such separate IRR database could be realized as a DCS itself. Furthermore, ROA entries could be added to the DCS as secure transactions and those transactions would be relied upon by route validators as authoritative. Perhaps DCS validation information could be added as a new ROA field.

In terms of openness of the system, a permissioned system would restrict both clients and miners to, e.g., AS owners, through suitable verification steps upon joining the DCS. A permissionless realisation, on the other hand, could more widely distribute the BGP origin information, still relying on the detection of fraudulent announcements through the above steps before executing a transaction.

A key requirement for realizing a suitable DCS for BGP is the latency requirement for achieving consensus, i.e., retrieving the latest valid information from the DCS. This requirement will need reflection in choosing the appropriate proof technique for consensus.

In the next section, we list several opportunities for using DCS in BGP by expressing those opportunities in smart contract language, i.e., allowing for being formulated as a distributed state machine with a distributed information pool representing the latest valid state of the system.

3. Opportunities for Using DCSs for BGP

There are various ways DCSs could be used in the context of BGP that we will explore in this section, keeping in mind the questions of the previous section.

3.1. Preventing fraudulent BGP origin announcements

BGP origin information is at the heart of BGP to ensure reachability in the global Internet, while preventing any fraudulent announcement of a BGP origin is an additional security aspect in providing this global reachability.

Announcements (of BGP origins) here represent smart contracts in a DCS, amending a distributed state (the BGP routing table), while securing those transactions prevents fraudulently doing so.

For anomaly detection purposes, we could further secure BGP origin information by comparing what's in a BGP blockchain table against what's in the BGP table or the forwarding table. Additional reliance upon BGP blockchain table could potentially help prevent high frequency updates from causing routing disruptions.

3.2. Validating incoming BGP updates

This is very similar to the previous aspect whereas BGP origin may not just be announced but updated, represented through a different state machine to manipulate the distributed BGP information in the DCS.

And according to RIPE labs, BGP route updates tend to converge globally in a few minutes. The propagation of newly announced prefixes happens almost instantaneously, reaching 50% visibility in under 10 seconds. Prefix withdrawals take longer to converge and generate nearly 4 times more BGP traffic, with the visibility dropping below 10% after approximately 2 minutes.

Although a DCS will likely not help with BGP updates, withdrawals may be completed faster than in existing BGP systems.

Furthermore, networking innovations that link DCS operations, like its ledger diffusion, more directly to emerging network capabilities, as suggested in [IIC whitepaper], may improve the DCS' transaction completion latency and thereby provide a suitable alternative even for update operations. This provides an opportunity for more research and testing.

3.3. Providing routing policy such as QoS

In addition to the prefix to AS match information being stored in the DCS, the routing policy of those routes could also be stored as part of the DCS information. As long as the policy was correctly added to the chain, the path policies cannot be altered except by those authenticated to do so.

3.4. Protecting BGP files

The DCS information could also be used to store configuration files within an AS in order to prevent malicious config tampering and to prevent misconfiguration.

This protection could be provided within a private, i.e., permissioned, DCS where only authorized users have access to the DCS data. This could also be used within a trusted external peering environment to build a distributed database of BGP files such as communities for use between BGP neighbors. Peers can use the DCS data to understand the necessary peering relationship and act on the communities in a consistent manner.

3.5. Providing path validation

BGP stores multiple paths to a destination in the BGP table. The BGP table contains all of the routes from all of the neighbors. Only the best route gets installed in the routing table. To help further secure the BGP table, all of those routes/paths could be installed in a DCS. Some mechanism could be used to validate these routes/ paths, that reside in the DCS, prior to one being selected as the path in the routing table. This could also be extended to provide proof of transit across certain expected paths.

3.6. Securing BGP Controllers

BGP-LS is used to provide BGP topology information to a Controller. That topology information could be added to a DCS to ensure that the topology data is not compromised. PCEP, or other protocol, could be used by a controller to validate any update of a BGP forwarding table using this same (or separate) DCS. The latest forwarding rules would be maintained in a DCS, which is built using BGP-LS data and authorized users as an input. Without the proper credentials it would be very difficult to update the forwarding rules in the DCS and a record would be kept with all update attempts.

Furthermore, the DCS could be permissisoned, thereby restricting the nodes holding as well as accessing information to trusted members of the community.

3.7. Securing Blockchain compromised by BGP vulnerabilities

The attractiveness of DCS applications, such as Bitcoin and Ethereum, are that they are highly decentralized and more resistant to attack. This has opened the way for securing monetary transactions using crytocurrencies and their underlying blockchain technology.

Blockchains mining power, however, is centralized with mining pools concentrating within certain regions and Autonomous Systems. This also creates a more centralized routing situation which could become vulnerable to BGP vulnerabilities where IP addresses of the mining pools are hijacked. Therefore helping to further secure BGP will help to secure blockchain's centralized mining pools, creating a circular dependency where the use of blockchains in BGP will in turn secure blockchains themselves.

4. Conclusions

This document discusses the use of distributed consensus system (DCS) techniques to complement and further secure BGP overall.

Although no specific recommendation on solutions is made, this document aims at providing first insights to think more broadly on a DCS-based infrastructure that may further enhance the capabilities of BGP as a key protocol for the Internet.

5. IANA Considerations

N/A

6. Security Considerations

There could be new blockchain related attacks that BGP would experience if blockchain were to be added into BGP's policy system. These attacks include trying to replace the trusted chain with a fradulent chain. We will explore some of those here or in a new draft.

7. Acknowledgement

8. Normative References

[IIC_whitepaper] Trossen, D., Guzman, D., Kelkar, A., Fan, X., McBride, M., Zhang, L., and U. Graf, "Impact of Distributed Ledgers on Provider Networks", Whitepaper Industry IoT Consortium Whitepaper, 2022, <https://www.iiconsortium.org/pdf/2022-01-10-Impact-of-Distributed-Ledgers-on-Provider-Networks.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI

10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

Authors' Addresses

Mike McBride
Futurewei

Email: michael.mcbride@futurewei.com

Dirk Trossen
Huawei

Email: dirk.trossen@huawei.com

David Guyman
Huawei

Email: david.guzman@huawei.com