

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 29 October 2022

M. McBride  
Futurewei  
27 April 2022

BGP Blockchain  
draft-mcbride-rtgwg-bgp-blockchain-00

## 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 29 October 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

BGP Blockchain

April 2022

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Requirements Language . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Proposed Blockchain for BGP solutions . . . . .	<a href="#">3</a>
<a href="#">2.1.</a>	Blockchain to prevent fraudulent BGP origin announcements . . . . .	<a href="#">3</a>
<a href="#">2.2.</a>	Blockchain to validate incoming BGP updates . . . . .	<a href="#">3</a>
<a href="#">2.3.</a>	Blockchain to provide routing policy such as QoS . . . . .	<a href="#">3</a>
<a href="#">2.4.</a>	Blockchain to protect BGP files . . . . .	<a href="#">3</a>
<a href="#">2.5.</a>	Blockchain to provide path validation . . . . .	<a href="#">4</a>
<a href="#">2.6.</a>	Blockchain for BGP Controllers . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Blockchain compromised by BGP vulnerabilities . . . . .	<a href="#">4</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">4</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">5</a>
<a href="#">6.</a>	Acknowledgement . . . . .	<a href="#">5</a>
<a href="#">7.</a>	Normative References . . . . .	<a href="#">5</a>
	Author's Address . . . . .	<a href="#">5</a>

## [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 Blockchain to secure BGP? This document provides a review of how Blockchain could be used to secure BGP particularly as supplemental 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 Blockchain to BGP is that it adds additional security without changes to the BGP protocol. 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.](#) Proposed Blockchain for BGP solutions

There are various ways Blockchain could be used to help secure BGP that we will explore in this section.

### [2.1.](#) Blockchain to prevent fraudulent BGP origin announcements

Prefix origin announcements could be stored on a blockchain to avoid BGP human configuration errors or hijacks. The consensus algorithms will ensure that everyone knows the correct owner AS of the prefix and everyone will know if there is an unauthorized change attempt. The existing RPKI system could be used to to authorize prefix owners and then an additional step could be to treat that as a transaction to be stored on a blockchain. ROA entries could be added to a blockchain as secure transactions and those transactions would be relied upon by route validators as authoritative. Perhaps blockchain validation information could be added as a new ROA field.

### [2.2.](#) Blockchain to validate incoming BGP updates

This is very similar to the previous solution. If using RPKI, route validators could cross check with the BGP blockchain before sending authorized prefix/AS matches to relying BGP routers. If not using RPKI, then routers would need to check a IRR blockchain prefix/AS database, if one were to exist, in order to validate incoming BGP updates.

### [2.3.](#) Blockchain to provide routing policy such as QoS

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

### [2.4.](#) Blockchain to protect BGP files

Blockchain 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 blockchain environment where only authorized users have access to the blockchain 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 data in the blockchain to understand the necessary peering relationship and act on the communities in a consistent manner.

### [2.5.](#) Blockchain to provide 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 blockchain. Some mechanism could be used to validate these routes/paths, that reside in the blockchain, prior to one being selected as the path path in the routing table. This could also be extended to provide proof of transit across certain expected paths.

### [2.6.](#) Blockchain for BGP Controllers

BGP-LS is used to provide BGP topology information to a Controller. That topology information could be added to a blockchain 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) blockchain. The latest forwarding rules would be maintained in a distributed blockchain 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 blockchain and a record would be kept with all update attempts.

## [3.](#) Blockchain compromised by BGP vulnerabilities

The attractiveness of Blockchain 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 cryptocurrencies 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.

#### 4. IANA Considerations

N/A

McBride

Expires 29 October 2022

[Page 4]

---

Internet-Draft

BGP Blockchain

April 2022

#### 5. 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 fraudulent chain. We will explore some of those here or in a new draft.

#### 6. Acknowledgement

#### 7. Normative References

[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>>.

Author's Address

Mike McBride  
Futurewei  
Email: michael.mcbride@futurewei.com