POSTER: BGPCoin: A Trustworthy Blockchain-based Resource Management Solution for BGP Security

Qianqian Xing, Baosheng Wang, Xiaofeng Wang
College of Computer, National University of Defense Technology
Changsha, Hunan, China 410073
xingqian0110@hotmail.com,bswang@nudt.edu.cn,xf_wang@nudt.edu.cn

ABSTRACT

Origin authentication is one of the most concentrated and advocated BGP security approach against IP prefix hijacking. However, the potential risk of centralized authority abuse and the fragile infrastructure may lead a sluggish deployment of such BGP security approach currently. We propose BGPCoin, a trustworthy blockchain-based Internet resource management solution which provides compliant resource allocations and revocations, and a reliable origin advertisement source. By means of a smart contract to perform and supervise resource assignments on the tamper-resistant Ethereum blockchain, BGPCoin yields significant benefits in the secure origin advertisement and the dependable infrastructure for object repository compared with RPKI. We demonstrate through an Ethereum prototype implementation that the deployment incentives and increased security are technically and economically viable.

CCS CONCEPTS

• **Security and privacy → Security protocols**;

KEYWORDS

Blockchain; BGP security; Origin authentication; RPKI

ACM Reference format:
Qianqian Xing, Baosheng Wang, Xiaofeng Wang. 2017. POSTER: BGPCoin: A Trustworthy Blockchain-based Resource Management Solution for BGP Security. In *Proceedings of CCS'17, Oct. 30–Nov. 3, 2017, Dallas, TX, USA., ,* 3 pages.
DOI: http://dx.doi.org/10.1145/3133956.3138828

1 INTRODUCTION

RPKI [3] and ROVER [7] both provide a PKI-based trusted mapping method from an IP prefix to the Autonomous System(s) (ASes). Although RPKI has been advocated and standardized of the relevant protocols by IETF, the potential misconfigured, faulty or compromised RPKI authorities may result to its disappointingly sluggish adoption [2]. ROVER claims a "fail-safe" mode to protect BGP from misconfigurations, but it has no help to hinder the misbehavior of centralized authorities. Despite the efforts of appending logs to visualize and alarm changes to the RPKI passively, and providing consent for revocations to balance the power of RPKI authorities positively [3], they still suffers from the following problem: (1) RPKI and ROVER do not sufficiently incentivize recording or monitoring authority behavior, (2) to achieve the revocation consent in RPKI or ROVER requires such a complicated and burdened collaboration between RC issuers(to sign) and relying parties(to validate) that may also lead to its passive application, (3) RPKI's infrastucture is fragile to resist the deleting and overwriting of objects from malicious authorities and maintain a consistent view of information (RCs, ROAs, manifests).

In summary, we have reasons to debate that RPKI or ROVER neither gives an efficient and reliable solution to extricate ISPs from IP hijackings or takedowns.

For the inherently untrusted and error-prone Internet, the blockchain is an ideal trustworthy and reliable infrastructure [1] supporting security architectures. We propose BGPCoin, a trustworthy blockchain-based resource management solution. Concretely, (1) BGPCoin compels every authority organisation to operate compliant resource assignments and revocations(under consent) by a smart contract, thus primarily precludes the misconfigurations and entity misbehaviors (that violate to the contract), (2) the append-only ledger on the blockchain maintains a consistent view of information in BGPCoin, which not only avoids mirror world attack like in RPKI, but also forbids reversing or overwriting the resource assignments.

2 BGPCOIN DESIGN

BGPCoin is a system hosted on the Ethereum blockchain and controlled by a smart contract, that allows entities to manage (such as storing, allocating, assigning and revoking) Internet address and Autonomous System Number resources of itself and other participants, i.e., the Internet Assigned Numbers Authority(IANA), Regional/National/Local Internet Registries, Internet Service Providers(ISPs) and Autono-mous Systems(ASes). Instead of origin authorization by RCs and ROAs, BGPCoin records resource assignments and authorizations in transactions on the Ethereum blockchain [5]. By tracking changes of the ownerships and usufructs of resource assets through a public ledger created and maintained through network consensus, every resource is solely owned or leased.

BGPCoin Infrastructure: In contrast with RPKI that requires different components to sign/store/verify origin attestations, BGPCoin only need the existing Ethereum system as its infrastructure, including its Ethereum blockchain and the miners. We retain the Bitcoin notion of addresses, peers, miners, transactions, blockchains. Every participated entity peer with its address as its public key has it own private keys (as a key-pair with its address).

(1) BGPCoin Miner vs. Relying Party: Compared with that RPKI objects are cryptographically verified by their relying parties, the

CCS'17, Oct. 30–Nov. 3, 2017, Dallas, TX, USA.
ISBN 978-1-4503-4946-8/17/10.
DOI: http://dx.doi.org/10.1145/3133956.3138828

task of verifing a transaction is in charge of the BGPCoin contract and the miners. Once a transaction is added to the blochchain, its verification has been confirmed. Compared with that RPs push origin validation results to edge routers to inform routing decisions in BGP, BGPCoin allows an edge router to directly request IP resource mappings from the Ethereum client in its own AS.

(2) Blockchain vs. Repository: Different with the distributed repositories which are undertaken by their authories without supervision, the Ethereum blockchain provides a distrubuted and tamper-resistant log of all transactions, leading to transaction non-repudiability and the ability to retrace the history of any transaction. Thus the global consistent view of information in BGPCoin avoids mirror world attack[3] like in RPKI.

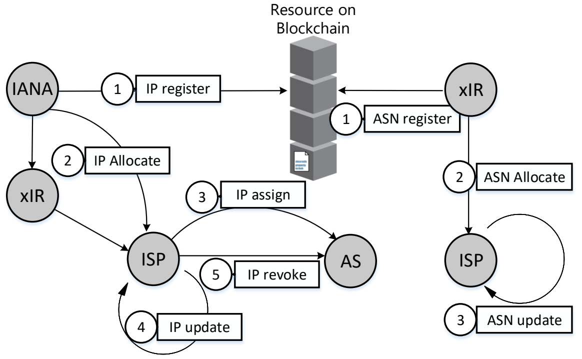

Figure 1: Operators for IP and AS number resource in BGPCoin. xIR represents RIR, NIR and LIR which are respectively short for Regional/National/Local Internet Registry.

BGPCoin Components: The design of BGPCoin contains two primary components: the smart contract which dictates the protocol of the system and acts as an interface to the blockchain for the resource management, and the client which interacts with the smart contract to allow users to fully utilize the system by allowing them to search for resource. The contract of BGPCoin contains two primary functions, **resource trading** and **resource searching**, with one characteristics: **aggregated Internet Address repositing&updating**. The resource management protocol for BGP security is implemented by operating the BGPCoin resource trading function. The client of BGPCoin complishes every IP validation according to the IP ownership record on the blockchain by operating the resource searching function. For the efficient storage by compressing the amount of resource entries on blockchain, BGPCoin aggregates the IP-Prefixes that are contiguous and have the same owner and the same leasee (in the case that they are leased).

2.1 Smart Contract

The smart contract defines all operations that the participated entities can take upon the assets and also the precondition and the result of those operations. An entity refers to any participant in the system, i.e., IANA, xIPs and ISPs. BGPCoin has two types of assets: *Internet Address resource* and *AS numbers resource*. Every asset has its fields to represent its assignment and authorized status, shown in Fig.1, which as the origin attestation supports IP announcement validation in BGP updating.

```
struct IPB{                 struct ASNData
   uint32  IP_start;           {
   uint8   wildnum;             address owner;
   State   state;               uint    IPBindex;
   address owner;               uint    stime;
   address leasee;              uint    validperiod;
  }                            }
   mapping (uint24 => ASNData) public ROA;
```

Figure 2: Data Structures of BGPCoin Assets.

BGPCoin has three types of *entities* and five types of *trading operations* for *Internet Address resource*: IANA for registering IP resources and allocating to xIRs, xIRs for allocating IP resources to its sub xIRs and then to ISPs, ISPs for allocating IP resources to its sub ISPs or assigning them to ASes, and three types of *trading operations* for *AS numbers resource*: RIRs for registering ASN resources and allocating to its sub xIRs or ISPs, as shown in Table.1 and Fig.1. We note that an IP resource assignment means an established lease with its period of validity. The owner of some resource has the right to update the resource after its period of validity. IP revoke operated by its owner in its period of validity is only allowed on the condition that a consent signature of the resource leasee is appended.

Table 1: Semantics of BGPCoin trading operations

Operation	Example
IP register	IANA:$< IPB, \varnothing >$
IP allocate	IANA/xIR→xIR: $< IPB, \varnothing >$
IP assign	xIR:$< IPB, ASN >$
IP update	xIR:$< IPB, ASN_1 > \to < IPB, ASN_2 >$
IP revoke	xIR:$< IPB, ASN > \to < IPB, \varnothing >$
ASN register	xIR:$< ASN, -, - >$
ASN allocate	xIR→ISP:$< ASN, stime, period >$
ASN update	ISP:$< ASN, stime', period >$

2.2 Client

Every resource authority organization maintains an Ether-eum client to interact with the smart contract to not only take operations upon its own resource, but also retrieve resource data from the blockchain.

Prior-setting. As the deployer of BGPCoin, IANA firstly collects the mappings from all resource authority organizations to their Ethereum account addresses. The mappings authorized by every participated organization (IANA, xIRs and ISPs) are collected as a profile in the contract before BGPCoin is launched. As a result, one transaction between Ethereum accounts, as an attestation, could be mapped to a resource allocation from its present owner to its next owner, or a resource assignment from its owner to the leasee.

Route Origin Advertisement. Every AS maintains an Ethereum client to the contract. Compared with the method of downloading the validated ROAs list from rely parties in RPKI, ours allows an edge router to directly request IP resource mappings from the Ethereum client in its own AS.

3 BGPCOIN TRANSACTION VS. RC/ROA IN RPKI

The BGPCoin and RPKI both protect against prefix and subprefix hijacks by providing a trusted mapping from an IP prefix to an AS

Table 2: BGPCoin Transaction vs RC/ROA

Transaction in BGPCoin		RC/ROA in RPKI	
History-based trustworthiness	Sequential Transparency	Certificate-based trustworthiness	Log-appending Transparency
	Hash-chained Integrity		Menifest-signed Integrity
Transaction Audit	Miner Verification	Unbridled Authority Misbehavior	Misconfiguration
	Immutable Ledger		Stealthy Deleting/Overwriting
	Muti-signature Consent		Unilateral Revoke/Reclaim
Explicit Resource Ownership	Sole Usufruct of IP prefix	Overflexible Resource Attestation	Double-cover IP prefix
	Reallocation after Withdrawal		Targeted Whacking

Table 3: Cost of BGPCoin trading operations

Operation	Gas	USD	Operation	Gas	USD
IP register	155448	0.259	IP revoke	72960	0.121
IP allocate	188113	0.313	ASN register	42411	0.071
IP assign	183246	0.305	ASN allocate	68876	0.114
IP update	69101	0.115	ASN update	27691	0.046
BGPCoin Contract Creation				3985649	6.631

authorized to originate the prefixes in BGP. In contrast to RC/ROA in RPKI, BGPCoin transaction yields significant benifits with three properties detailed in Table 2.

History-based trustworthiness: The history-based trustworthiness supported by the blockchain not only frees BGPcoin from certificate management, but also essentially plays a role of the monitor and log system which comparatively is an additional assembly in RPKI.

Inherent transaction audit: The conduction of BGPCoin smart contract with the miner verication eradicates the misconfigurations and entity misbehaviors that violating to the contract like stealthy deleting/overwriting objects. The immutable ledge on blockchain guarantees that once a resource transaction is successfully validated by miners, it is impossible to reverse or overwrite it. Moreover, muti-signature consent precludes the unilateral revoke. Those inherent transaction audit property enables BGPRoin to eliminate the risk from authorities.

Explicit resource ownership: Explicit resource ownership indicated by the transaction ledger eliminates the circular dependency[2] in issuing RCs(or ROAs), since a transaction concurrently displays an allocation(or assignment) and its authorization.

4 EVALUATION

We has implemented a working prototype of BGPCoin. We implement the smart contract in Solidity[1], a high-level Ethereum language that resembles JavaScript for writing smart contracts that are compliled to EVM code. We demonstrate the preliminary experiment upon Truffle[2], a development environment and testing framework for Ethereum.

Preliminary Results: We estimated the approximate computational steps (in Ethereum's gas) and approximate costs (in US dollars, for creating the BGPCoin contract and for each trading operation supported by the BGPCoin contract in Table 3.As in May 2017, 1 ether =$92.43 and 1 gas= 1.8×10^{-8} ether [3]. We note that the cost of the operations in Ethereum is relatively low compared with the fee-of-service internet resource management. Moreover, the participated organization motivates the mining and validation by increasing the mining reward and fee on demand when submitting a resource transaction.

Scalability. A BGP peer receives 4.94 average prefix updates/s [4]. Since Ethereum has 7-15 trans/s[4] and moreover, adavanced consensuses[5] are in progress to promote the Ethereum's thrughputs to thousands transactions per second, that is viable to have BGPCoin averagely 5 tran/s throughput for BGP advertisement.

5 CONCLUSION AND FUTURE WORK

In this work, we introduce a novel Internet resource management solution for BGP security. We design the BGPCoin system consisted with a smart contract-based resource assignment attestation and a blockchain-based dependable repository infrastructure. We demonstrate through a preliminary analysis that the deployment incentives and increased security are technically and economically viable. We are conducting extensive experiments to study the scalability of the global deployment of BGPCoin and the security enhancement [6] of the smart contract of BGPCoin. We believe BGPCoin poses the feasible and credible BGP security solution on the condition of the security of Ethereum blockchain itself and the smart contract programming. Other security threat similar of vulnerable loose ROAs [2] in RPKI are considering to be forbidden in the future by a rigorous route policy for BGP adversiments in BGPCoin.

ACKNOWLEDGMENT

This research is supported in part by the project of National Basic Research and Development Program of China (2012CB315906), and National Key Research and Development Program of China (2017YFB0802301).

REFERENCES

[1] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. 2015. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *Security and Privacy.* 104–121.

[2] Yossi Gilad, Avichai Cohen, Amir Herzberg, Michael Schapira, and Haya Shulman. 2017. Are We There Yet? On RPKI's Deployment and Security. In *NDSS.*

[3] Ethan Heilman, Danny Cooper, Leonid Reyzin, and Sharon Goldberg. 2014. From the consent of the routed: Improving the transparency of the RPKI. In *Proceedings of the 2014 ACM conference on SIGCOMM.* ACM, 51–62.

[4] Geoff Huston. 2017. The BGP Instability Report. (2017). http://bgpupdates.potaroo.net/instability/bgpupd.html.

[5] Daniel Kronovet. 2017. A next-generation smart contract and decentralized application platform. (2017). https://github.com/ethereum/wiki/wiki/White-Paper.

[6] Loi Luu, Duc Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. 2016. Making Smart Contracts Smarter. In *ACM Sigsac Conference on Computer and Communications Security.* ACM Press, 254–269.

[7] Aanchal Malhotra and Sharon Goldberg. 2014. RPKI vs ROVER: comparing the risks of BGP security solutions. In *SIGCOMM 2014 ACM conference.* ACM Press, 113–114.

[1] http://solidity.readthedocs.io/en/develop/index.html

[2] https://github.com/trufflesuite/truffle

[3] https://ethstats.net/, https://coinmarketcap.com/.

[4] https://en.wikipedia.org/wiki/Ethereum

[5] https://github.com/ethereum/EIPs/issues/225