The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet

Adiseshu Hari T.V. Lakshman
Nokia Bell Labs, USA
{firstname.lastname}@nokia.com

Abstract

Existing security mechanisms for managing the Internet infrastructural resources like IP addresses, AS numbers, BGP advertisements and DNS mappings rely on a Public Key Infrastructure (PKI) that can be potentially compromised by state actors and Advanced Persistent Threats (APTs). Ideally the Internet infrastructure needs a distributed and tamper-resistant resource management framework which cannot be subverted by any single entity. A secure, distributed ledger enables such a mechanism and the blockchain is the best known example of distributed ledgers.

In this paper, we propose the use of a blockchain based mechanism to secure the Internet BGP and DNS infrastructure. While the blockchain has scaling issues to be overcome, the key advantages of such an approach include the elimination of any PKI-like root of trust, a verifiable and distributed transaction history log, multi-signature based authorizations for enhanced security, easy extensibility and scriptable programmability to secure new types of Internet resources and potential for a built in cryptocurrency. A tamper resistant DNS infrastructure also ensures that it is not possible for the application level PKI to spoof HTTPS traffic.

1. INTRODUCTION

The Internet infrastructure is designed to operate amongst a set of cooperating Autonomous Systems (ASes) and be administered via a set of cooperating Internet registries. This assumption of cooperative entities needs to be re-examined in today's world of Advanced Persistent Threats (APTs), state actors, cyber terrorism and cyber warfare, in which the ASes and Internet registries themselves might be compromised. Attacks on the core Internet infrastructure such as the Domain Name System (DNS) and the BGP Internet routing protocol can bring the entire Internet to a standstill, or cut countries and continents off from it.

Currently, Internet resources like IP addresses and domain names are administered at the top level by regional Internet registries (ARIN, APNIC etc.). Most countries also operate their own registries via delegation from the regional registries. This lets them manage IP address allocation to local ISPs and DNS servers for their country specific DNS domains. Once this administration of IP addresses to individual ASes is done, the ASes advertise their IP prefixes via BGP Update messages which are propagated around the Internet.

Each regional and country specific registry, as well as each AS can potentially be breached, leading to compromised DNS resolution and BGP routing. There exist mechanisms to secure IP address assignments to ASes via digitally signed transactions using an Internet Resource specific Public Key Infrastructure called the RPKI [34], as well as PKI methods to sign DNS records (DNSSEC [5]), but as in any PKI based scheme, these schemes are vulnerable if the root of trust is compromised. For the same reason, signed BGP Update messages based on RPKI signatures as proposed by BGPSec [2] do not solve the AS-Path verification problem.

What the Internet infrastructure needs is a distributed, tamper-resistant, peer to peer (p2p) infrastructural resource management mechanism outside the control of any single entity. This mechanism should let Internet peers such as ASes and DNS domain owners verify ownership of *Internet infrastructural resources* such as IP prefixes and domain names of other Internet peers and verify the *Internet transactions* that each peer attempts such as transferring domain ownership or advertising Internet paths to an IP prefix. A secure, distributed resource transaction ledger enables such a mechanism. While many distributed p2p consensus mechanisms such as Paxos [32] and PBFT [21] have been proposed in literature, the most popular mechanism for building a secure, distributed transaction ledger amongst untrusted peers today is the blockchain pioneered by the Bitcoin [35] cryptocurrency. In this paper, we propose a blockchain based distributed ledger solution to secure infrastructural BGP and DNS transactions without the need for any PKI.

While the Bitcoin blockchain was designed to record cryptocurrency transactions, in this paper we describe the use of

HotNets-XV, November 09 - 10, 2016, Atlanta, GA, USA

 ISBN 978-1-4503-4661-0/16/11…$15.00

DOI: http://dx.doi.org/10.1145/3005745.3005771

a Bitcoin like blockchain for Internet resource transactions. We call such a blockchain the *Internet blockchain*. Just as the Bitcoin blockchain provides a verifiable record of Bitcoin transactions and thus prevents Bitcoin misuse such as double spending, the Internet blockchain can record Internet core transactions like IP address assignments, domain name assignments and AS-Path advertisements, thus allowing Internet peers to verify core Internet resource usage and assignment authorizations. We discuss the operation of the Internet blockchain in depth in the next section. While popular in a number of applications, the blockchain does have major scaling issues which is the subject of much current active research and is discussed further in Section 4.

1.1 The Blockchain as a Distributed Transaction Ledger

We assume familiarity with the operation of the Bitcoin blockchain [35, 19], but we review some basic concepts here. The blockchain is secured by public key cryptography, with each peer generating its own public-private key pairs. In the blockchain p2p system, peers have blockchain addresses, which are hashes of their self generated public cryptographic keys. *Unlike PKI, a peer does not need to get its address authenticated by any other entity or CA, thereby eliminating the possibility of key tempering or spoofing by a third party.* A blockchain transaction involves a resource transfer from one or more *inputs* to one or more *outputs*. The blockchain transaction outputs refer to blockchain addresses and specify the amount of resources transferred to that output. The blockchain transaction inputs are pointers in the form of cryptographic hashes to the outputs of previous blockchain transactions and redeem the resources specified in those outputs via digital signature based proof of ownership of the blockchain addresses (public keys) specified in those outputs. We emphasize again that blockchain address of a peer does not refer to its IP address, but a hash of its public key. Once a blockchain transaction output is referenced, it can no longer be referenced again, thereby preventing double spends. Thus a blockchain transaction provides a secure resource transfer framework to move resources from one or more blockchain addresses to one or more blockchain addresses.

Transactions are broadcast to the p2p network. These transactions are verified and periodically aggregated into blocks by p2p network peers called miners. These mined blocks are broadcast back to the p2p network, where each peer collects them into a linear chain of blocks called the blockchain. Transaction verification by miners and peers is simple. Since each transaction input points to previous transaction outputs, as long as those previous transactions are present in blocks incorporated into the blockchain and the corresponding outputs have not been already referenced, the current transaction is considered valid. Since any Bitcoin peer can be a Bitcoin miner and all transactions can be verified by all peers, a compromised miner which puts out fake or double transactions in a block will be detected immediately by the peers. As a result, the Bitcoin network is resistant to compromised peers or miners, thus enabling decentralized transactions across untrusted peers. Figure 1 shows two transactions (the blockchain is not shown), with the first transferring 5 units of a resource from A to B and the second transaction showing the resource being transferred from B to C.

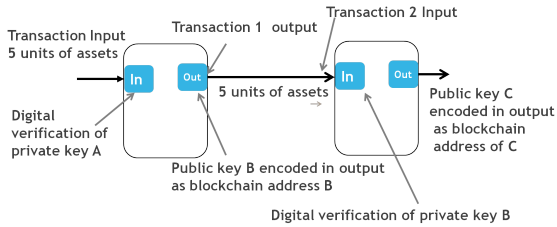

Figure 1: Blockchain Transaction moving 5 units of a resource from A to B to C

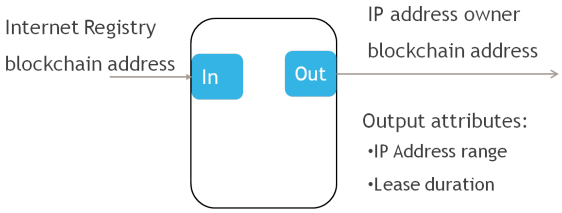

Figure 2: Genesis transaction for IP address allocation

1.2 Blockchain Properties Desirable for Internet Transactions

We are now in a position to understand the appeal of abstracting and extending the blockchain to provide a tamper-resistant Internet resource transfer mechanism without a centralized PKI style root of trust. First, all transactions occur between peers without any mediation. No intermediary or PKI is needed for verification of resources being transferred since the verification is based on the transaction history linking the inputs of the current transaction to the outputs of prior transactions that are recorded in the blockchain. By replacing a PKI based root of trust with a root of trust based in a globally shared ledger, the blockchain eliminates the potential for root of trust violations by state actors and cyber criminals. Second, the blockchain provides a distributed and tamper-resistant log of all transactions, leading to transaction non-repudiability and the ability to retrace the history of any transaction.

Third, a transaction can be secured using not just a single key, but multiple keys. This is shown in Figure 3 which shows Transaction 1's output being assigned to a 2 of 3 multi-sig blockchain address The multi-sig address specifies not one, but three different standard blockchain addresses and also specifies the number of signatures required to redeem it,

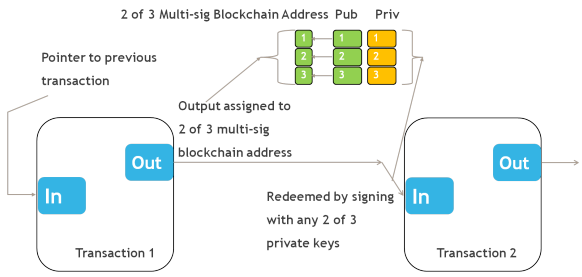

Figure 3: 2 of 3 Multi-sig Transaction

which is two in this case. Thus, Transaction 2 needs to be signed by two of the three private keys corresponding to the blockchain addresses. In the general case, *N* of *M* multi-sig addresses are supported. This greatly enhances security if the private keys are stored separately, since an attacker would need to discover not just a single private key, but multiple ones to redeem the transaction. This is in contrast to the multiple signature algorithms present in DNSSEC, where any one algorithm can be used. This corresponds to a 1 out of *N* multi-sig scheme. Multi-sig transactions also allow for a peer to survive a key loss, as well as a mechanism for gradual key rollover.

Fourth, the ability of a transaction to have multiple inputs and multiple outputs provides a very compact representation of complex transactions compared to traditional one-to-one transactions. Fifth, it is possible to associate a cryptographic currency with the blockchain. This atomically couples resource transfer and payment in a single transaction. It also enables transaction fees, thereby creating a payment incentive for miners and imposing a cost on gratuitous transactions.

2. TAMPER-RESISTANT TRANSACTION FRAMEWORK

In this section we describe how to derive the Internet blockchain for securing Internet infrastructure resources, starting from the Bitcoin blockchain. We retain the Bitcoin notion of addresses, peers, miners, transactions, blocks and blockchains in the Internet blockchain, but the Internet blockchain is a new data structure that is completely separate from the Bitcoin blockchain. The Internet transactions do not deal with Bitcoins, but with Internet infrastructural resources like IP addresses, AS numbers, DNS names and BGP path advertisements. While the Bitcoin blockchain is designed with some added considerations, such as pseudonymity and Bitcoin creation in mind, for the purposes of the Internet blockchain, we only use the feature of transactions being able to reference multiple previous transactions and create multiple outputs.

The goal of the Internet blockchain is to preserve the consistency of the Internet resources on a day to day basis without mediation, even if one or more of the Internet entities is compromised. In particular, subversion of top level entities such as Internet registries or the DNS root zone by state actors should not cause existing IP prefix assignments or DNS names or BGP advertisements to be either revoked or spoofed — a critical feature missing from the current PKI based Internet security frameworks.

2.1 Internet Blockchain System Model

In our model, existing Internet registries, ASes and DNS domain owners act as peers in the Internet blockchain, each with its own Internet blockchain address and corresponding private key. There is an initial *genesis* bootstrap period in which the current official Internet resources are transferred into the Internet blockchain in the form of one of more genesis blocks, with each block consisting of multiple transactions, with each transaction recording the transfer of an Internet resource from a registry to Internet entities. Once the genesis blocks are created, all Internet resources are published to the Internet blockchain and this provides an initial consistent state of the Internet resource allocation. At this point, each entity is free to publish new Internet transactions to the p2p network, and each entity is free to mine Internet transactions into blocks in the Internet blockchain. The Internet registries will continue to function and make new resources available on the blockchain, but will lose the ability to revoke or spoof previously assigned resources at will. Both the genesis transactions, as well as subsequent ones, can be multi-sig, e.g., requiring multiple Internet registries to sign a transaction (to prevent unilateral assignment), or allowing an AS to use one of multiple signatures.

2.2 Incremental Deployment Scenario

It can be argued that the Internet blockchain is too big and too disruptive for global deployment. We therefore outline an incremental deployment scenario where its benefits can be realized on a smaller scale to begin with. An Internet blockchain can expand in scope along two dimensions. First, there is the resource scope where more and more resource types are secured. Here, the blockchain can first start with RPKI functionality, such as recording IP address ownership and Route Origin Authorizations (ROAs [33]), proceed to BGPSec like BGP advertisement transactions, and finally provide DNSSEC like DNS transactions. Second, there is a geographical scope where more and more enterprises and ASes join the blockchain. Here, the blockchain can begin as an intra-enterprise or intra-cloud distributed ledger of BGP transactions. This is useful in scenarios such as BGP based SDN controller peering [10] where BGP is used to provide reachability information across network controller instances. From intranets, it can expand to extranets where the federating controllers are from different organizations, e.g., at an Internet Exchange(IX) or SDX [29]. It can then expand to cover multiple cooperating IXes and finally expand to cover the entire Internet. We describe below the resource scope based deployment scenario.

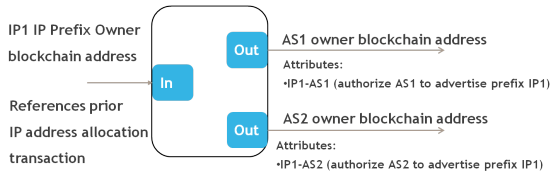

Figure 4: Route Origin Authorization (ROA) Transaction from a multi-homed site

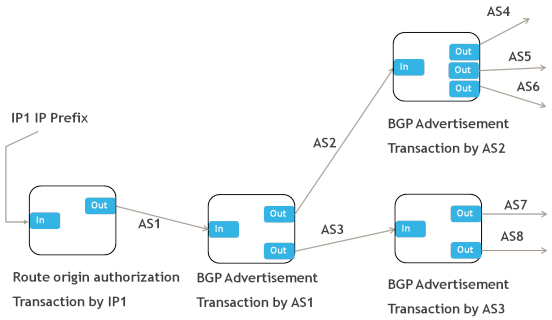

Figure 5: BGP Advertisement Transactions

2.3 New Transaction Types

The genesis blocks enable all Internet entities to accurately map Internet resource ownership. The infrastructural resources we consider are IP addresses and prefixes, AS names, Route Origin Authorizations (ROAs [33]) and DNS domains. The genesis blocks allow us to verify if a particular entity owns an IP address prefix, if a particular entity owns a given AS number, if a particular AS is allowed to advertise a particular prefix in BGP (Route Origin Authorization) and if a particular entity is allowed to delegate a particular DNS domain. Since the Internet transactions specify the resource type, it is possible for peers on the Internet blockchain to verify their validity and to prevent double spend like transactions. For example, if the IP address prefix 25.0.0.0/8 has been previously assigned to address A by a registry with address B, an attempt to create a new transaction to assign this prefix to address C will fail by anyone other than address A. Figure 2 shows a genesis transaction for IP address allocation, and Figure 4 shows an ROA from a multi-homed site authorizing AS1 and AS2 to advertise its IP prefixes. This provides an example of a compact multi-output transaction. Each transaction also has a *transfer tag*, indicating whether the resource can be transferred to another entity. For example, a registry might reset the transfer tag for IP prefixes assigned to ISPs, preventing the ISPs from transferring the prefixes to others. Most Internet infrastructural resources are leased, not owned. A resource lease is modeled by adding a *lease duration* field in resource transfer transactions and with a second reverse transaction that transfers the resource back to the original owner but is dated at the lease expiry, so it will come into effect only at that time.

2.4 Recording BGP Advertisements

We now focus on the issue of recording external BGP (eBGP) transactions in the Internet blockchain to provide BGPSec-like functionality. With the previous extensions, we have seen how the Internet transactions can verify RPKI-style Internet resource usage authorization. For example, if an AS X advertises that it is directly connected to IP prefix Y, then the Internet blockchain can tell us the true owner of Y and whether the owner of Y had authorized AS X to advertise this prefix. This is very useful to prevent IP hijacking and false BGP advertisement at the origin. However, this does not solve the case of false BGP advertisements further downstream. In this case, a BGP speaker might be 5 AS hops away from an IP prefix, but might advertise a 2-hop AS-path to the prefix.

To solve this type of false downstream BGP advertisement, we need to record all BGP advertisements by all BGP speakers in the Internet blockchain in a new type of transaction called the *BGP advertisement* transaction. Each time a BGP speaker advertises an AS-Path to an IP prefix in a BGP Update message, it also creates a corresponding BGP advertisement transaction and publishes it to the Internet blockchain p2p network. Each advertisement blockchain references its previous upstream AS in its inputs from whom it originally received the BGP update, and all its downstream ASes in its outputs to which it is sending an Update message referencing this AS-path. There is also a corresponding *BGP withdraw* transaction to withdraw a previously advertised AS-path if necessary.

For example, assume AS1 initially advertises IP Prefix IP1 to AS2 and AS3. In that case, AS1 will create a BGP advertisement transaction listing the ROA transaction for IP prefix IP1 as its input and AS2 and AS3 as its outputs as shown in Figure 5. Other entities can thereby verify from the blockchain that AS1 is allowed to advertise prefix IP1, and that AS2 and AS3 have received this advertisement from AS1. Subsequently, if AS2 advertises this path to AS4, it will create an advertisement transaction listing the transaction received from AS1 as the input and AS4 as the output. However, if AS4 were to advertise this path in BGP as AS4-AS1-IP Prefix IP1, then its BGP peers can easily verify that AS4 is not capable of sending packets to IP prefix IP1 via AS1, since the advertisement transaction by AS1 only lists AS2 and AS3 as recipients of the prefix IP1, not AS4.

Recording BGP advertisements on the blockchain raises dependency issues not present in RPKI and BGPSec. We have a circular dependency between BGP routing and the Internet blockchain, with each dependent on the other. To ensure a shared fate for both the advertisement transactions and the BGP Update messages, each AS exchanges BGP advertisements in the form of blockchain transactions rather than Update messages. This is shown in Figure 6 which shows a BGP to blockchain converter module in front of each BGP

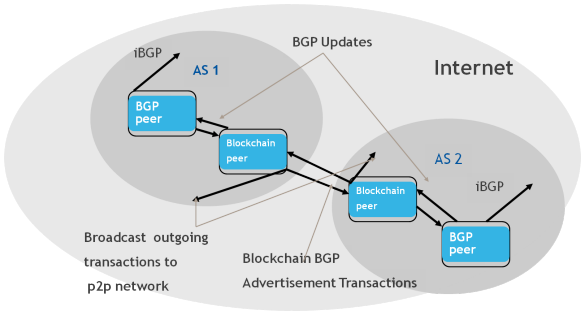

Figure 6: Integrating BGP Updates with BGP Advertisement Transactions

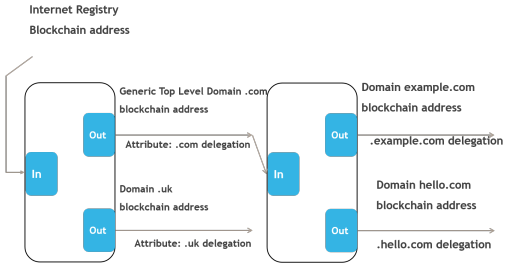

Figure 7: Transaction chain for DNS delegation

speaker. The blockchain converter module takes outgoing BGP Updates and converts them into advertisement transactions which are broadcast on the blockchain p2p network as well as sent to the next AS, where the corresponding module converts them back into BGP Updates for the BGP speaker to process. Thus, no changes to the BGP protocol or implementation are required. Note that there is no information loss as both provide the same semantic information. This arrangement ensures that the BGP Updates and the blockchain advertisements are always in sync, which is not possible if both are exchanged in parallel. Note that blocks are published only periodically to the blockchain, while BGP needs to act immediately on incoming transactions. Hence for fast convergence, each BGP speaker needs to speculatively accept incoming transactions before they are published to the blockchain.

2.5 Recording DNS Transactions

In this section, we describe how DNS requests, such as the DNS name to IP address mapping can be validated using new Internet blockchain transactions, thereby providing the security equivalency of DNSSEC [5]. DNSSEC associates each DNS domain with a public key called the DNSKEY and enables tamper-resistant DNS queries by requiring the domain name servers to use the DNSKEY to sign responses to DNS requests. Similar to RPKI and BGPSec, we aim to provide Internet blockchain equivalent transactions for DNSSEC. The transaction we introduce is the *DNS domain delegation* transaction, which transfers a sub domain from one entity to another as shown in Figure 7. Note that the DNS domain delegation transaction is distinct from the transactions on the Namecoin [9] blockchain, which provides a DNS-like name to address mapping. Unlike Namecoin, which provides the equivalent of DNS A records in a private .bit namespace, the Internet blockchain provides proof of ownership of public DNS domains in the DNS hierarchy. As the domain delegation transaction that created a specific domain also provides the domain's blockchain address as its output, the domain's blockchain address can serve as the DNSKEY for the domain. Since all DNS domains originate from the DNS root domain, we can therefore trace a domain's validity in the blockchain via the domain delegation transactions to the root domain creation transaction in the genesis block.

A major advantage of using the blockchain address of a domain to validate its domain records is that we can eliminate the domain and name validation provided by application level PKI and Certificate Authorities (CAs), similar to the DNSSEC based authentication scheme proposed by DANE [8]. Crucially, it is no longer possible for a CA to spoof a domain as the spoofed domain keys will not match the keys recorded in the DNS delegation blockchain transaction This secures application level HTTPS and other PKI secured traffic from tampering (though not certificate revocation). While all domains on the Internet blockchain are publicly visible, private domains, e.g., the internal subdomains of an enterprise, do not need to be put in the blockchain as they are not publicly accessible.

3. EXTENSIONS

Our initial goal has been to replicate the functionality provided by RPKI, BGPSec and DNSSEC. It can be argued that a disruption to the Internet architecture such as the Internet blockchain, should provide much greater functionality than simply replacing existing security frameworks. For example, we could couple BGP advertisement transactions with fine grained per-flow routing directives. The main reason we do not do so is to preserve the existing stability and convergence properties of the Internet, which is based on existing protocols and frameworks. For example, both the blockchain and BGP have the ability to recover from network partitions, so by using a relatively unmodifed blockchain with BGP-like transactions, we can retain similar recovery and convergence properties.

We note that the Internet blockchain transactions can always be extended to provide more functionality. For example, transaction output validation in the Bitcoin blockchain is provided by a rudimentary scripting language. This has been enhanced to become a full fledged programming languages in other blockchains like Ethereum [14]. Hence it is possible to enhance the Internet blockchain to provide fully scriptable transactions which trigger only when some specified events occur, e.g., a BGP route which is advertised only when a particular path exceeds a specified capacity.

We can also potentially couple a cryptocurrency with the

Internet blockchain. Adding a currency to a blockchain is straightforward and is in fact the primary motivation of the Bitcoin blockchain. An associated cryptocurrency makes transaction payments both convenient and atomic. It also incentivizes the Internet blockchain and its mining, since the payments can also cover the transaction fees and ensure that peers that generate large transactions pay larger fees.

4. SCALABILITY AND RELATED WORK

Blockchain Implementation Issues

The primary implementation issue with a blockchain is its scalability. Is it possible to create an Internet wide blockchain with the bandwidth necessary to support huge numbers of transactions? The transaction rate supported by a blockchain is fundamentally limited by the periodicity with which blocks are added and the limit on the size of each block, making it more suitable for reads than writes. For example, the Bitcoin blockchain adds a block every 10 minutes with a maximum blocksize of 1 MB, thereby limiting the bitcoin transaction rate to between 3 and 7 per second, based on the size of individual transactions on the blockchain [1, 4]. On the other hand, a typical 1 week period on the Internet [13] shows a BGP peer receiving a peak of around 9000 prefix changes/s superimposed on the daily BGP churn [24]. This means that to be viable the Internet blockchain needs to have more than 4 orders of magnitude higher transactional throughput just for BGP advertisement transactions alone. Numerous research proposals seek to address the blockchain scaling problem. Bitcoin-NG [25] is a proposal to use leader election to select the miner of the *next* block, rather than the current block, ensuring that current transactions are continuously processed. We can also speed up the consistency of the blockchain as described in [23, 22] to reduce the impact of speculative acceptance of BGP advertisements. Sidechains [17] and Payment Channels [11] are hierarchical solutions that move transactions off the parent blockchain. For example, the DNS and BGP transactions could reside on separate blockchains off a parent RPKI blockchain. The Hashgraph [6] is a new scalable, byzantine fault tolerant, distributed consensus protocol that eliminates the need for proof-of-work for mining by linking all the blocks into a new interlinked data structure called the hashgraph.

Beyond scalability, another blockchain issue is potential denial-of-service attacks caused by large mining pools as seen in Bitcoin [3]. The Internet blockchain is designed to be run by a large number of high capacity, geographically distributed peers which are organizations rather than individuals, thus making it much harder for miners to collude.

Blockchains and the Internet

The Hyperledger Project [15] seeks to create a standard blockchain for global business transactions. Blockstack [18], similar to Namecoin, is an example of a naming and identity solution, but instead of using a blockchain to provide naming for the Internet, it provides a name to blockchain address mapping for the Bitcoin blockchain. The Internet of Things (IoT) has sparked interest in using blockchain based technologies to automate the interconnections and servicing of IoT devices [7].

BGP Verification, Privacy, Extensibility and Security

NetReview [30] creates a secure log of BGP traces which can then be used to analyze BGP faults. The procedure for creating a secure log very nearly mimics the blockchain. NetReview focuses on posteriori fault detection, but with a blockchain based BGP transaction log, it is possible to do live fault avoidance.

In the current Internet, by default a BGP advertisement is only visible to downstream ASes unless an AS along the path chooses to explicitly share it, e.g. via a public database like Route Views [16]. However, the Internet blockchain inverts this default privacy by allowing all entities to view BGP transactions. It is possible to encapsulate the entire set of input transactions into a single mega transaction which can then be encrypted. Such a scheme, while workable, would impose severe costs in terms of block storage and transaction size and would be opaque to miners. This blowup in either transaction size or transaction computation [28] appears inevitable for privacy protection schemes.

An example of providing functionality beyond traditional BGP is described in [27], which describes a policy language for authorizing per-flow forwarding at an SDX. This is orthogonal to the Internet blockchain since the Internet blockchain provides a public log of each peer which can then be used by higher level logic systems to detect policy violations. There exists a considerable body of work delving into BGP insecurities and the efficacy of RPKI and BGPSec, e.g., [31, 26, 12, 20]. The primary consensus is that native BGP is insecure, but RPKI and BGPSec have the potential for misuse by state actors and lack an incentivizing mechanism for global deployment.

5. CONCLUSIONS

In this paper, we have described the Internet blockchain which creates a tamper-resistant framework for Internet infrastructural resource transactions by eliminating any PKI dependency or a root of trust. While the Internet blockchain is primarily driven by the need to counteract malicious state actors, it provides a host of other advantages, such as a built in transaction log for analyzing failures, multi-signature based authorizations for enhanced security, easy extensibility and the potential for a built in cryptocurrency as an incentivizing mechanism.

Clearly, blockchain scalability is an impediment to the adoption of the blockchain. However, blockchain scalability is an area of intense, active research and it is likely that the scalability issues will be addressed, thus enabling a blockchain based tamper-resistant Internet.

6. REFERENCES

[1] 7 Transactions Per Second? Really? http://hashingit.com/analysis/33-7-transactions-per-second.

[2] BGPSec Protocol Specification. https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-17.

[3] Bitcoin Mining Pools. http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html?_r=0.

[4] Bitcoin Scalability. https://en.bitcoin.it/wiki/Scalability.

[5] DNS Security Extensions. https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

[6] Hashgraph. http://www.swirlds.com/wp-content/uploads/2016/06/2016-05-31-Overview-of-Swirlds-Hashgraph-1.pdf.

[7] IBM ADEPT. http://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf.

[8] IETF DANE WG. https://datatracker.ietf.org/wg/dane/charter/.

[9] NameCoin. https://namecoin.info.

[10] Nuage Networks. http://www.nuagenetworks.net.

[11] Payment Channels. https://en.bitcoin.it/wiki/Payment_channels.

[12] Secure BGP Deployment Final Report. http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_202013.pdf.

[13] The BGP Instability Report. http://bgpupdates.potaroo.net/instability/bgpupd.html.

[14] The Ethereum Project. www.ethereum.org.

[15] The Hyperledger Project. https://en.wikipedia.org/wiki/Hyperledger.

[16] University of Oregon Route Views Project. www.routeviews.org.

[17] Adam Back et. al. Enabling Blockchain Innovations with Pegged Sidechains. https://blockstream.com/sidechains.pdf.

[18] M. Ali, J. Nelson, R. Shea, and M. J. Freedman. Blockstack: A Global Naming and Storage System Secured by Blockchains. In *2016 USENIX Annual Technical Conference (USENIX ATC 16)*, pages 181–194, Denver, CO, June 2016. USENIX Association.

[19] Arvind Narayanan et.al. Bitcoin and Cryptocurrency Technologies. https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1.

[20] J. Bailey, D. Pemberton, A. Linton, C. Pelsser, and R. Bush. Enforcing RPKI-based Routing Policy on the Data Plane at an Internet Exchange. In *Proceedings of the Third Workshop on Hot Topics in Software Defined Networking*, HotSDN '14.

[21] M. Castro and B. Liskov. Practical Byzantine Fault Tolerance. OSDI '99, 1999.

[22] C. Decker, J. Seidel, and R. Wattenhofer. Bitcoin Meets Strong Consistency. In *Proceedings of the 17th International Conference on Distributed Computing and Networking*, pages 13:1–13:10, 2016.

[23] Eleftherios Kokoris Kogias et. al. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 279–296, 2016.

[24] A. Elmokashfi and A. Dhamdhere. Revisiting BGP Churn Growth. *ACM SIGCOMM Computer Communication Review*, 44(1), 2013.

[25] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse. Bitcoin-NG: A scalable blockchain protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 45–59, 2016.

[26] S. Goldberg. Why Is It Taking So Long To Secure Internet Routing? *Communications of the ACM*, 57(10):56–63, 2014.

[27] A. Gupta, N. Feamster, and L. Vanbever. Authorizing Network Control at Software Defined Internet Exchange Points. 2016.

[28] D. Gupta, A. Segal, A. Panda, G. Segev, M. Schapira, J. Feigenbaum, J. Rexford, and S. Shenker. A New Approach to Interdomain Routing Based on Secure Multi-Party Computation. Hotnets'12.

[29] Gupta, Arpit et. al. SDX: a software defined internet exchange. *ACM SIGCOMM Computer Communication Review*, 44(4):551–562, 2015.

[30] A. Haeberlen. NetReview: Detecting When Interdomain Routing Goes Wrong. NSDI, 2009.

[31] E. Heilman, D. Cooper, L. Reyzin, and S. Goldberg. From the consent of the routed: Improving the transparency of the rpki. *ACM SIGCOMM Computer Communication Review*, 44(4):51–62, 2015.

[32] L. Lamport. The Part-Time Parliament. *ACM Transactions on Computer Systems*, 16(2), 1998.

[33] M. Lepinski et. al. A Profile for Route Origin Authorizations (ROAs). RFC 6482 (Proposed Standard), 2012.

[34] M. Lepinski et. al. An Infrastructure to Support Secure Internet Routing. RFC 6480 (Informational), 2012.

[35] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.