Blockchain and DNS: Improving Security

Abraham Flores

ICTN 4040

April 10, 2019

Abstract

DNS technology acts as the backbone of the internet but suffers from serious vulnerabilities that have been used in major attacks. These attacks include the Mirai botnet DDoS attack on DYN's DNS services, and the BGP/DNS poisoning of Amazon's route 53 service. By using blockchain technology as an underlying mechanism, DNS could have improved integrity and security, and using the peer-to-peer network, complete decentralization. There are already technologies providing DNS-like services using blockchain and can be looked to for an example of implementing DNS on a blockchain-based network.

Technologies we use every day come from older standards, that suffer from vulnerabilities inherent to them. One example of such technologies would be DNS, sometimes called the “backbone of the internet.” This technology suffers from a few vulnerabilities, ones that could be solved by introducing newer technologies to provided added security and integrity. One such technology that could improve DNS would be blockchain technology. Blockchain provides much-needed decentralization and provides a better way of “trusting” DNS sources. Blockchain is a relatively new technology but has older roots. It has recently come to increased attention due to its use in cryptocurrency but has many other potential uses. This paper will discuss how blockchain works, a few issues with DNS that could be resolved with blockchain, examples of attacks on DNS servers using these issues, and how blockchain could be used to eliminate or mitigate these issues.

Blockchain technology is based on two separate parts working together, for which it is named. The “block” data structure, and the “chain” that joins them. The “block” is where the main data in the blockchain is stored. It is a discrete structure containing a header, the data to be stored, and closing with a so-called “proof of work.” This proof of work is the basis of trust in the blockchain, and it creates integrity and immutability in the chain. Starting with the data in the block, the actual contents of it depends on the purpose of the chain. For cryptocurrencies, it is a list of transactions between wallets. For DNS purposes, this data can essentially be the same as normal DNS records. Once the header and data are in the block, “miners” begin their work. They compute hashes for the block, appending a string to the end of the block to meet certain requirements. These requirements depend on the specifications of the chain, and the difficulty. For

example, the chain could require the first 32 characters in the hash string be “0”. Thus, miners run calculations, changing their string and hashing the whole block until one is found that satisfies the requirement. Once a string meets the criteria, the miner sends out the completed block to the rest of the network. Other participants in the network verify the hash, and add the new block to their local ledger, re-sending it to their peers. The hash of this new block becomes the header for the next block. This is how the “chain” is formed. Even though a block is added to the chain, it is not yet accepted. A different chain could grow faster than the one the block was added to. At any given moment, several possible ledgers/chains could be floating throughout the network as blocks are transmitted peer to peer. However, in the end, the longer chain (the one with the most “work” in it) is the one that is adopted. This usually means that once four or five additional blocks are added past any given one, the one is then able to be trusted. Due to the computational complexity of generating a new hash, it becomes mathematically infeasible to change or remove a past block in the ledger. If someone wanted to do this, they would have to create a new hash for the block they are changing (or the block before it if removing one), as well as all blocks that have come since. Additionally, they would have to create enough hashes for new blocks faster than the entire rest of the network to get their false chain longer. In order to even stand a chance of falsifying a record, an attacker would have to have over 50% of the network’s computational capability [1].

Currently, DNS suffers from a few issues, but two specifically that could be solved with the use of blockchain are DNS poisoning and that DNS servers act as single points of failure. DNS poisoning is when an attacker creates false DNS records and either

propagates them to legitimate servers or hacks into and sets them directly on a legitimate server. This is usually for phishing purposes but could also serve as censorship among other reasons. This issue shows examples of a lack of integrity in DNS and can be attributed to the fact that trust in DNS simply comes from a centralized source saying so. However, this central source is not without flaw and is susceptible to attack, creating this vulnerability. Another issue with DNS also stems from this centralization, creating a potential single point of failure for users. If a large enough DNS provider is hit with an attack, it could create an issue not only for users, but for other DNS servers that rely on the larger one. Both these issues could be solved using blockchain technology. The ledger creates trust using the proof of work, while also providing decentralization, eliminating single points of failure by spreading the DNS records throughout the network.

Both mentioned problems with DNS have been put into practice in major attacks. DNS poisoning was used in the Amazon Route 53 attack, where attacks not only provided false BGP routes, but also managed to create false DNS entries to phish users of the Ethereum cryptocurrency. The falsified entries were there for two hours, and the attackers managed to get an estimated $150,000 worth of Ethereum by phishing users [2]. The single point of failure was a big issue during the DYN DNS attack using the Mirai botnet. Many major websites went down, including “Twitter”, “Etsy”, “Github”, “Spotify”, and “Soundcloud”, among others [3]. The issue went on for an initial two hours and was followed with a second attack that lasted for another hour [4]. These attacks took advantage of vulnerabilities that are unavoidable with current implementations of DNS and show a need for improvement and change.

The issues stated with DNS could be resolved using blockchain technology. With blockchain, a network could be established where users generate their keys for creating entries. They then mine others' blocks to add DNS entries, and as a reward, are permitted to create their own. As stated earlier, the chain provides trust and integrity, and acts as an immutable ledger of all DNS records. This isn't to say a record couldn't be updated later – it just means that the updated record must come in a later block, and the older block with the outdated record will forever exist in the chain. Additionally, a new block would need to have the same source in order to be accepted as a valid "transaction", meaning not just anyone can update a record. The entire network acts as a failsafe against single points of failure. Every peer participating in the network has their own copy of the ledger, and it can be shared with non-participants who trust a source to provide it without having to join the network. Of course, if no such source exists, anyone is free to join the network themselves and have the entire ledger available to them.

Of course, blockchain technology does not come completely without challenge. Due to the current way of issuing domains through centralized locations, it would be hard to just move to a decentralized platform. Someone could join the network and try to claim a domain that is already owned by someone else. This issue, however, could be resolved by using a system similar to PGP, where users have their keys signed by other users who trust them [5]. This avoids having to centrally authenticate any given key while maintaining trust that a key is who they say they are.

Two good examples of blockchain technology being used in DNS and DNS-like systems today would be the so-called "Blockchain DNS" and the "Ethereum Name

Service". Blockchain DNS is a service that provides DNS entries for domains with a top level domain of ".bit", ".lib", ".emc", ".coin", and ".bazar", as well as domains using the OpenNIC infrastructure [6]. Anyone can download a custom software client that allows them to get their own copy of the ledger containing all the DNS entries, and are then able to connect to said domains. Alternatively, if one does not want to download the whole ledger but has a known trusted source server that is in the network, they can simply use that server as a normal DNS server. The Ethereum Name Service doesn't exactly provide DNS service, but rather provides a similar service that translates a name like "alice.eth" to an Ethereum wallet address, which is otherwise 42 hexadecimal characters long [7]. It works on the same principal as Blockchain DNS, distributing the ledger among many people. Both of these services, to provide incentive for people to join the network as well as have entities to perform the "mining" to add new blocks to the chain, require new users to provide a certain amount of work in order to fully join the network or add a block/entry of their own. Obviously, this is not a requirement, as one can still get these services by utilizing a trusted server that already exists on the network.

As explained, DNS is a widely used technology and acts as the backbone of the internet. It is not, however, without flaw. These flaws provide major attack vectors for anyone to take advantage of. These flaws, centralization and poisoning, have already been used in major attacks, and will most likely be seen again in more focused ones. These vulnerabilities could be solved by adopting blockchain technology into DNS. It would provide a peer to peer network for decentralization, and immutability to avoid poisoning.

References

* [1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. [Online] Available: https://bitcoin.org/bitcoin.pdf [Accessed April 10, 2019].

[2] D. Goodin, “Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency,” Ars Technica, 24-Apr-2018. [Online]. Available: https://arstechnica.com/information-technology/2018/04/suspicious-event hijacks-amazon-traffic-for-2-hours-steals-cryptocurrency/. [Accessed: 10-Apr 2019].

[3] B. Chacos, “Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline,” PCWorld, 21-Oct-2016. [Online]. Available: https://www.pcworld.com/article/3133847/ddos-attack-on-dyn-knocks-spotify twitter-github-etsy-and-more-offline.html. [Accessed: 10-Apr-2019].

[4] DYN, “Update Regarding DDoS Event Against Dyn Managed DNS on October 21, 2016,” Oracle Dyn Status History Atom, 21-Oct-2016. [Online]. Available: https://www.dynstatus.com/incidents/5r9mppc1kb77. [Accessed: 10-Apr-2019].

* [5] E. Karaarslan and E. Adiguzel, "Blockchain Based DNS and PKI Solutions," IEEE Communications Standards Magazine, vol. 2, (3), pp. 52-57, 2018.

[6] “Blockchain DNS: First Step Towards the Uncensored Internet”, BDNS, 2017. [Online] Available: https://blockchain-dns.info/ [Accessed April 10, 2019].

[7] “Ethereum Name Service,” Ethereum Name Service, 2016. [Online]. Available: https://ens.domains/. [Accessed: 10-Apr-2019].