

Review of blockchain-based DNS alternatives

HU Wei-hong¹, AO Meng¹, SHI Lin², XIE Jia-gui¹, LIU Yang²

(1. Beijing Teleinfo Network Technology Co., Ltd., Beijing 100095, China;

2. China Academy of Information and Communication Technology, Beijing 100191, China)

Abstract: DNS Protocol was originally designed with no security protection in place. Subsequent DNSSEC added a layer of trust on top of DNS by providing authentication, but it still did not address issues such as DoS/DDoS attacks and deployment difficulties. Blockchain technology offers an innovative perspective to tackle those challenges. By reviewing and analyzing two prevail blockchain-based DNS alternatives (Namecoin and Blockstack), it is concluded that although blockchain presently have problems that have to be solved, it is a promising approach to build decentralized, secure and human-friendly naming systems.

Key words: DNS, DNSSEC, decentralization, blockchain, Bitcoin, Namecoin, Blockstack

doi: 10.11959/j.issn.2096-109x.2017.00157

1 Introduction

The domain name system (DNS) was born in the Internet's early days when the network was primarily used for academic and military purposes. The design of its distributed hierarchical structure made the system simple, scalable and resilient. Presently this system has been deployed almost on every computer in the world, which proves that this design philosophy successfully serves its purposes. However, there is one factor that was not top of the designers' mind: security, because they never anticipated the Internet could be world widely adopted in the future. As a result, this DNS system is fundamentally vulnerable since its invention and was bothered by all kinds of security issues as the Internet continually develops. The most common one is named distributed denial of service (DDoS) attack. Most recently, in October, 2016, DDoS attacked the servers of Dyn^[1], a company that controls much of the Internet's DNS infrastructure, bringing down websites including Twitter, Netflix, Reddit, CNN and many other in the US and Europe. This attack is roughly twice as powerful as any similar attack on

record, which makes it the largest of its kind in history. Other than DDoS which attacks DNS servers, there are several security vulnerabilities oriented from the flaws in the DNS protocol such as DNS cache poisoning and man in the middle attack which also threaten the security of DNS.

Efforts to shore up DNS are ongoing. One such effort is the domain name system security extensions (DNSSEC) which aims to address these issues by adding security to DNS protocol while maintaining backward compatibility. DNSSEC was designed to provide DNS clients origin authenticated information and to prevent DNS data from being forged or manipulated, which makes it an effective weapon against attacks such as DNS cache poisoning. Basically, in a DNSSEC deployed zone, the DNS answers clients received are digitally signed. By checking the digital signature, clients are able to know whether the data contained in the answers is altered. Although DNSSEC guarantees the authentication and integrity of DNS data, it does not provide confidentiality of data, which means all DNSSEC data are not encrypted and visible to everyone. Another negative effect of DNSSEC is that

the signing and verification of DNS data introduce additional overhead to the servers and network, thereby impacting the performance of DNS servers and making them more vulnerable to DDoS attacks. The complexity and difficulties of DNSSEC deployment also hinder the adoption. Additional workloads are placed on system administrators and organizations and the benefits that arise from this cost are not incentive enough for them to deploy DNSSEC.

DNS was designed as a distributed database which enables it to scale and perform efficiently under variety of conditions. Despite the fact that DNS servers are distributed all over the world, DNS is also a centralized system in terms of administration and redundancy. All of those distributed components operate in reference to a central authority which could be viewed as a centralized point of failure. For example, the root zone is managed by IANA/ICANN, the former of which is administrated by the US government. On the other hand, the centralized hierarchy structure of current DNS exposes vulnerabilities to DDoS attack such as previously mentioned attacks to Dyn. Therefore, decentralized DNS is probably one direction to solve these issues. Tor^[2] is a secure and decentralized system, but its primary objective is to achieve anonymity as opposed to decentralization. Therefore, the lack of capability of using human-meaningful names impedes its further adoption. Blockchain is another recently emerged technology which could be a promising solution to all the challenges DNS systems are facing. In this paper, several blockchain-based DNS alternative systems are reviewed and compared. Meanwhile, their merits and potential limitations are also discussed and analyzed.

2 Background

2.1 Blockchain

Bitcoin^[3] is a typical blockchain-based proto-

col, and probably is the most successful application of blockchain technology so far. Thus, we take Bitcoin as an example to brief some fundamental concepts of blockchain prior to the discussion of blockchain-based DNS protocols.

Bitcoin's self-explanatory name indicates that Bitcoin is a digital cryptocurrency. Fundamentally, it is a decentralized payment system which consists of four key components.

1) The underlying network structure on which the system operates.

2) The essential activity occurring in the system: transaction.

3) Distributed public ledgers which keep track of all transactions.

4) A mechanism which decides who is authenticated to record and verify transactions.

Network: Unlike other centralized or hierarchical networks, the Bitcoin network is a peer-to-peer (P2P) payment network that operates on a cryptographic protocol. Nodes can join and leave the network freely. Transactions are broadcast to all nodes using a flood protocol. Messages are delivered on a best effort basis. Through the use of P2P network, the transaction database is managed autonomously. Every node keeps a copy of transaction database locally and no centralized official copy exists. Upon joining the network, a new node bootstraps itself by downloading and verifying data from other nodes to complete its local copy.

Transaction: As a digital currency, the basic functionality of Bitcoin is circulating in the system. A certain amount of Bitcoin transferred from one user to another forms a transaction. The sender issues a transaction/payment by signing it with its private key. Then the transaction will be spread through the network and every node receiving it will verify the signature using the sender's public key. Eventually the transaction reaches a legitimate bookkeeper (aka. miner) where it is queued for further processing.

Blockchain: The database which consists of all transactions is organized by blocks. Each block contains the hash of the previous one, making the database a chain of blocks, namely block chain. In a block, every transaction has a hash associated with it. The data integrity is secured by Merkle root which is the hash of all the hashes of all the transactions in the block. It is noteworthy that in the Bitcoin system, there is no such concept that one can stash unspent money somewhere on/off the block chain. This information can be gained by tracing back all the historical transactions related to this person.

Mining: In the Bitcoin system, there are plenty of nodes who are willing to do the bookkeeper job because they can gain rewards for verifying and recording transactions. However, to maintain global consensus in the whole system, only one node is elected to create a new block and package transactions into it. This election process involves solving a math problem. Whoever first finds the solution becomes the leader and has the authority to generate a new block which will be filled with pending transactions and broadcast to all nodes. Other nodes accept the new block only if the transactions within it are valid. Then, they can start working on the math problem for the next new block. The election process is named “mining” and the participants are miners.

2.2 DNS security

For a domain name system, one can identify its security level using RFC 3833^[4] which is originally created to determine if DNSSEC meets the security goals. In this subsection, some well-known DNS attacks are briefly described and will be utilized to evaluate the security of blockchain-based DNS systems discussed in next section.

As the DNS primarily relies on unencrypted UDP packets to carry information, there is no guarantee for end-to-end data integrity. It is easy for an attacker to intercept the DNS traffic or alter the

DNS data (modifying the answer to refer to another IP, or returning an NXDOMAIN code which tells the client that the domain does not exist) using a man-in-the-middle attack. Common DNS attacks such as DNS cache poisoning, DNS ID hacking and DNS spoofing fall into this category, namely DNS protocol attack.

As many other Internet services, the DNS is vulnerable of DoS/DDoS attacks. The attack target is DNS servers in place of the weakness of DNS protocol. A DoS attack is a malicious attempt to make a server or a network unavailable to users usually by sending a flood of requests to a server. When the load exceeds capacity, the server will not be able to respond to normal requests. In DDoS attacks, a network of computers infected with special malware are coordinated into bombarding a server with traffic until it collapses under the strain. This type of attack is the one of the hardest to defense against in the Internet.

There is another attack whose direct target is neither DNS protocol nor DNS servers. Most network devices send DNS queries to a trusted recursive resolver which can be arranged by network providers via DHCP protocol. If the trusted server is compromised or the client is configured to use a malicious resolver, for example, by attacking DHCP servers, DNS queries will be sent to attackers who may respond with whatever they want.

2.3 Zooko's triangle

Zooko Wilcox-O'Hearn proposed that there are three properties that are generally desired to have in a naming protocol^[5].

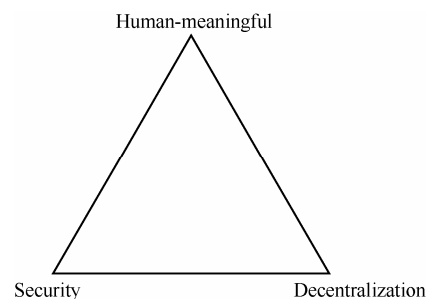


Fig.1 Zooko's triangle

1) Human-meaningful: the name provided to users should be meaningful and easy to remember and write without errors.

2) Secure: a name can only be resolved to one, unique and correct entity, even in the presence of untrusted nodes.

3) Decentralized: no central authority in the system and untrusted nodes are probably present.

He conjectured that in a key-value system in which the keys address values, compromise must be made between those three properties. In other words, you may have at most two out of the three properties in the system. This claim has been used to evaluate where a system stands on the evolution path to a perfect naming system. For example, the DNS name is human usable but the system is not distributed or secure. DNSSEC addresses the security issue on the top of DNS, therefore it has two properties except decentralization. Another example is the Tor naming system, which is secure and distributed, but the addresses are not human-meaningful. Fortunately, Wilcox-O'Hearn's claim was conjecture and is not necessarily correct. It is possible that naming systems are able to possess all three properties, or at least approach the third. Such systems will be discussed in the following sections.

3 Blockchain-based DNS alternatives

3.1 Namecoin

Namecoin^[6] is the first blockchain-based DNS system. It is a fork of Bitcoin with modifications which allow the blockchain to store name-value data other than transactions. Thus, Namecoin and Bitcoin share the most functionalities and mechanisms. For example, they utilize the same math problem for mining so miners are able to mine in both systems without consuming double computing power, aka. merged-mining. However, this may raise potential security risks which will be discussed in details.

Namecoin was designed as a more general name-value resolving system rather than a substitution of the current DNS system. In addition to the domain name, Namecoin can map other types of name-value pair which are differentiated by a prefix. For example, the “d/” prefix is used for domain names and “id/” is used to register identities. Namecoin uses the virtual .bit top-level domain name which is not officially registered in current DNS system. This means Namecoin is isolated from the DNS system and users cannot resolve .bit domain names without installing additional resolving software. Namecoin provides complete functionalities for registering, renewing and transferring a domain as traditional DNS does.

3.2 Blockstack

Blockstack^[7] is the first naming system which operates directly on top of the Bitcoin blockchain. Formerly it was Onename and built on top of Namecoin. After a security crisis of Namecoin, the development team decided to migrate the whole system to the Bitcoin blockchain. Therefore, the ability to migrate across different blockchains became one of their design philosophies and the name is also changed to Blockstack which reflects the concept of layered blockchains.

Feature-wise, Blockstack combines a DNS system with PKI (public key infrastructure). We skip discussing the latter as it is out of the scope of this paper. Both Namecoin and Blockstack share the similar DNS functionality with one major difference stemming from Blockstack's distinctive multi-layer blockchains. Namecoin stores name-value pair data on the blockchain. Thus, the maximum length of a domain name is 64 characters. Otherwise the blockchain will grow too fast. On the contrary, Blockstack is built on top of the Bitcoin blockchain which cannot accommodate large data such as name-value pair information. Therefore, a separate logical layer, i.e. virtualchain, on top of the blockchain is proposed to maintain the naming system

while the underlying blockchain is only used for achieving consensus on the state of the naming system and the integrity of name-value data records. Decoupling the naming system logic and consensus mechanism is a significant improvement over Namecoin. Not only can Blockstack increase the data storage capacity considerably, but allows the logical layer to improve and extend independently.

3.3 Nebulis and more

Another project similar to Blockstack is a platform called Nebulis^[8], a global distributed directory which intended to upgrade and replace the existing DNS using blockchain. The difference between the two is that their platform uses IPFS^[9] or MaidSafe^[10] as a replacement for HTTP and utilizes the Ethereum^[11] blockchain for DNS capabilities.

There are other blockchain-based naming systems such as Emercoin^[12] and EtherID^[13] which may focus on other aspects of a DNS system such as name squatting, pricing policies. These are more of social or economic issues than technical problems. Fundamentally they share the similar underlying technology with Namecoin or Blockstack.

4 Discussion and analysis

4.1 The advantages

In terms of Zooko's Triangle theory, blockchain-based DNS systems have all the three properties. They inherit most merits of decentralization as the underlying blockchain is natively decentralized. Unlike the current DNS which is administrated and controlled by an organization, there are no authorities in blockchain-based DNS. All the nodes equal to each other. Only owners can make changes to existing records with their private key. It is almost impossible for authorities to make changes to the domain name records.

With respect to security, blockchain-based DNS has obvious advantages as well. Traditional DNS is vulnerable to variety of attacks due to protocol flaws. Even with the enhancement of

DNSSEC, it still cannot thwart DoS/DDoS attacks. On the contrary, since all domain names are locally stored on every node, there is no need for the client to query the names by interacting with remote servers. Therefore, all the man-in-the-middle attacks present in traditional DNS no longer exist in blockchain-based DNS. The DoS/DDoS cannot impact the name resolution either because all the lookups are performed locally. Another benefit associated with local lookup is privacy protection. Traditional DNS/DNSSEC does not encrypt the data, which means it is visible to everyone and your privacy information (such as the websites you like and your usage pattern) is possibly exposed to malicious eavesdroppers.

In summary, blockchain-based DNS systems possess all the three properties for a naming system. They are immune to attacks traditional DNS usually suffers such as protocol attacks and server attacks. Additionally, they can offer privacy protection for the clients. It all looks like blockchain technology is a perfect solution for a naming system. But do blockchain-based DNS systems have any disadvantages? The answer is yes.

4.2 Problems still remain

Blockchain technology presents a new perspective on information security. Traditionally data is protected usually by building walls and isolating them from known attacks. This reactive approach may not be applicable in the increasingly connected digital society. A better strategy is building robust and resilient systems which can defense against any attack in a proactive manner. Bitcoin was originally designed as such a system. However, as the adoption of Bitcoin was increasingly widespread, shortcomings and security vulnerabilities gradually exposed.

51% attack: When Bitcoin was proposed, its security foundation was based on the "one-CPU-one-vote" mechanism, in which case it is nearly impossible that 51% of the voters are not honest.

Clearly the inventor of Bitcoin did not foresee the evolution in mining gears. Profit drives miners to upgrade their computing power. Various technologies have been used for mining such as CPU, GPU, FPGA and even ASIC. Furthermore, computing power can be united together, forming a “mining pool” to generate blocks more quickly and therefore individual miner can receive a portion of the reward on a consistent basis. The intention of mining pool sounds plausible. But when the computing power of a single pool approximates 50% of the entire computing power on the network, it may raise serious security concerns because the pool has the capacity to sabotage security and trust foundation of the system even if it intends not to do so. In late 2014, a mining pool consistently had more than 51% of the total computing power on Namecoin. And there was an even worse situation. Blockstack observed a mining pool controlled up to 75% of the computing power during a particular week, indicating Namecoin was actually controlled by a single party who was capable of undermining the security of Namecoin. This situation is probably caused by the “merged-mining” mechanism. A lot of profit-seeking large mining pools mine coins in both Namecoin and Bitcoin at the same time to maximize their profit. However, the rest miners only mine Bitcoin and they do not have incentive to mine other coins, which makes Namecoin less secure against 51% attack than Bitcoin. Due to this security concern, Blockstack migrated the whole system from Namecoin to Bitcoin. Nevertheless, the possibility of 51% attack still exists in Bitcoin system and it remains an open problem that needs to be addressed in the future.

Performance: The current Bitcoin protocol limits the generation rate of new blocks at 1 block per ten minutes or so, which makes the system can only accept up to 7 transactions per second. As more applications operate on Bitcoin, this will eventually become the bottleneck of Bitcoin and significantly

delay the confirmation of transactions. Increasing block size can mitigate this issue. But changing block size is a very complicated problem and the Bitcoin developers and communities are still debating its pros and cons. Modifying block size requires a hard fork, which mean if it is not adopted by almost all the nodes, Bitcoin could split into separate payment networks permanently. For a naming system built on top of Bitcoin, this is a difficulty which has to be tackled or circumvented. But if a naming system uses its exclusive blockchain, this is only a problem one needs to take into consideration when designing the system.

Last mile problem: Blockchain is a distributed system, meaning every node keeps a complete copy of blockchain data locally. As of Dec. 2016, the blockchain size of Bitcoin is 91 GB^[14] and still counting. For Namecoin, the blockchain size currently is 4.69 GB^[15] and it is expected that the size will significantly increase when scaling to millions of users in the future. Therefore, storing and maintaining massive blockchain data at every node might not be viable. For example, modern mobile devices such as smartphones usually do not have sufficient storage space for Bitcoin’s blockchain data. Moreover, messages and transactions are delivered in a flood fashion, which means mobile devices have to be waked up frequently to process received events thereby increasing battery consumption dramatically. Namecoin offered a tradeoff solution to balance decentralization and feasibility. Specifically, a node with full local copy of blockchain data can act as a traditional DNS recursive resolver by listening to port 53. Mobile devices can send DNS queries to this resolver for name lookup. However, this solution leaves data exchange between clients and resolvers unprotected like traditional DNS does. Previously mentioned DNS protocol attacks and server attacks become security threats again. This is the “last mile” problem for a blockchain-based DNS system, and is an area of future research.

5 Conclusion

Blockchain technology is an unstoppable force that could converge to a storm of computing revolution that would profoundly reshape not only businesses and societies, but also variety of Internet services. In this storm, blockchain-based DNS systems are forerunners of this Internet innovations from whom we can learn lessons. Essentially, blockchain technology is a candidate of great promise for the next generation DNS system in that it inherently possesses the qualities of censorship-resistance, security, and resilience. On the other hand, there still are issues such as 51% attack and last mile problem which have to be addressed by the endeavor of blockchain communities and researchers before blockchain-based DNS can be standardized and deployed in practice.

References:

- [1] Dyn Statement on 10/21/2016 DDoS attack[EB/OL]. <http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>.
- [2] DINGLELINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[J]. Journal of the Franklin Institute, 2004, 239(2): 135-139.
- [3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2009.
- [4] ATKINS D, AUSTEIN R. RFC3833: Threat Analysis of the Domain Name System (DNS)[J]. Internet Engineering Task Force, 2004, 5(1):108-117.
- [5] WILCOX-O'HEARN Z. Names: decentralized, secure, human-meaningful: choose two[EB/OL]. <https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html>.
- [6] Namecoin[EB/OL].<https://Namecoin.info>.
- [7] ALI M, NELSON J, SHEA R, et al. Block stack: a global naming and storage system secured by block chains[C]//2016 USENIX Annual Technical Conference (USENIX ATC 16). 2016: 181-194.
- [8] Nebulis[EB/OL].<https://www.nebulis.io/>.
- [9] IPFS (the InterPlanetary File System)[EB/OL]. <https://github.com/ipfs/ipfs>.
- [10] IRVINE D. MAIDSAFE.NET: US, EP2118808[P]. 2009.
- [11] Ethereum project[EB/OL]. <https://www.ethereum.org/>.
- [12] Emercoin [EB/OL]. http://emercoin.com/DNS_and_Name-Value_Storage.
- [13] Ethereum decentralized DNS[EB/OL]. <http://etherid.org/>.
- [14] Bitcoin blockchain size[EB/OL]. <https://blockchain.info/charts/blocks-size>.
- [15] Namecoin (NMC) statistics[EB/OL]. <https://bitinfocharts.com/Namecoin/>.

About the authors:



HU Weihong (1979-), born in Shannxi. He received his Ph.D. degree at University of California, Irvine. Currently he is with China Academy of Information and Communication Technology (CAICT). His research interests include the design and optimization of network protocols, the application and security of blockchain technology.



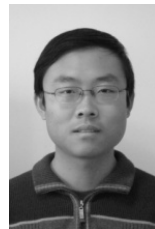
AO Meng (1982-), Daur nationality, born in Inner Mongolia. He received his Ph.D. degree at Institute of Automation, Chinese Academy of Sciences in pattern recognition and artificial intelligence in 2009. His research interests include artificial intelligence and blockchain technology.



SHI Lin (1988-), born in Shandong. He is an engineer at CAICT with years of experience in information security. Currently, he is the lead of trusted cloud security certification at institute of technology and standards research.



XIE Jiagui (1984-), born in Shandong. He received his Master degree at Institute of Automation, Chinese Academy of Sciences. Currently he is the CTO of Beijing Teleinfo Network Technology Co., Ltd., and his research interests involve DNS and intelligent information system.



LIU Yang (1986-), born in Gansu, PhD. He is a senior engineer at CAICT and the leader of the ID Working Group of AII (Alliance of Industrial Internet). His research focuses on industrial Internet, identification service and DNS.