Domain Name Management Architecture Based on Blockchain

Zhenjiang Ma(✉), Feng Qi, and Wenjing Li

Beijing University of Posts and Telecommunications, Beijing, China
mzj36900@bupt.edu.cn

Abstract. The centralization problem embodied in the domain name system (DNS) is getting more and more serious. It is not only vulnerable to network attacks but also suffered from abuse of authorities. Blockchain as an effective technical means which could solve decentralization problems brings light to the domain name system. We propose a domain name management architecture based on multi-blockchain. The architecture we proposed uses a relay chain to achieve the management of different top-level domain names. Compared with the single-chain system, the scalability and compatibility of decentralized DNS are improved. Besides, an off-chain storage method is designed for improving the throughput. Then we give the processes of domain name registration, modification, and resolution. Finally, the analysis and conclusions are given.

Keywords: Domain name system · Blockchain · Relay chain · Domain name management

1 Introduction

The domain name system maps domain names that are easy for a human to remember to IP addresses. The DNS is a vital infrastructure for all network applications. The centralized domain name system has been running well for decades, it has the advantages of high efficiency, good availability, and strong scalability. However, the centralization of the system is reflected in management and technical implementation, which leads to its weak robustness, poor security, and imbalanced power [1, 2].

The centralization of the DNS is embodied in three aspects. They are naming centralization, data-publishing centralization, and rolution centralization. The first two are involved in the management and the last one is involved in technology. Firstly, naming centralization means that a unified domain namespace is managed by The Internet Corporation for Assigned Names and Numbers (ICANN). Secondly, the data-publishing centralization means that domain name data is released by authoritative third-party organizations, so users do not have the right to dispose of digital assets (domain names). Thirdly, resolution centralization means that when the DNS is working, each domain name query begins from the root server which is vulnerable to a single failure.

This work was supported by grants from the National Key Research Program Projects (No. 2018YFB1800704).

S. Sun et al. (Eds.): ICSINC 2021, LNEE 895, pp. 303–309, 2022.
https://doi.org/10.1007/978-981-19-4775-9_37

In order to solve the problems of the invalid and untrustworthy resolution, Domain Name System Security Extensions (DNSSEC) is proposed [3], each domain uploads its own delegation signer (DS) record to the parent and the DS is signed by the parent, then a chain of trust is formed by signed DS record from root servers to other authority servers. There are drawbacks to DNSSEC: firstly, DNSSEC is based on asymmetric encryption which also introduces additional overhead during the encryption process. The computational overhead caused by DNSSEC message encryption will increase the workload of authority servers. In addition, the coverage rate of DNSSEC is low [4], unable to form the closure of the trust chain from the beginning to the end. Therefore, although DNSSEC is proposed, it cannot effectively solve the problem of untrustworthy resolution in the DNS.

Combining blockchain technology, we propose a new domain name management architecture, which uses the characteristics of multi-party participation and joint management of the blockchain to evolve the domain name system from a single-rooted tree-like structure into a multi-rooted net-like structure to realize decentralization of domain name management.

2 Background

The design of the DNS improves usability and efficiency. However, the system is vulnerable to DDoS attacks due to centralization, and there are also other security problems such as domain name pollution and hijacking. The composition and operation of the traditional DNS are as follows (Fig. 1).

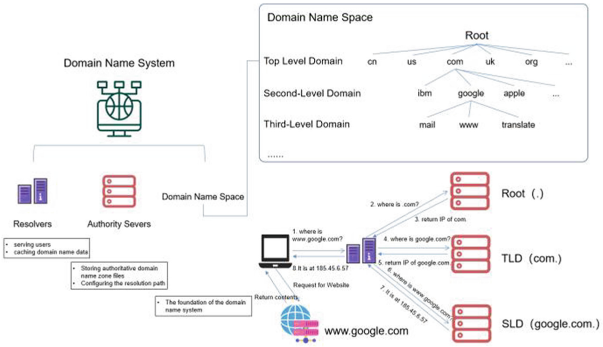

Fig. 1. Structure of domain name system

The blockchain originated from "Bitcoin: A Peer-to-Peer Payment System" published by Satoshi Nakamoto in 2008. It uses a blockchain structure to connect the front and rear blocks in series. Based on the irreversibility of the hash algorithm, it ensures credibility and resists tampering with the ledger data. Then the equal rights of participants are realized through the consensus algorithm. Blockchain uses consensus algorithms and cryptography to establish a trust system between unfamiliar users without an authoritative third party.

At present, there has been some progress in the research on the decentralization of the DNS. The decentralized DNS running on public blockchain includes Namecoin, Blockstack, Emercoin, Bitforest, and Ethereum's ENS. Among them, Namecoin is vulnerable to tampering due to its low computing power [5]. Blockstack proposes a four-layer architecture and is mounted on Bitcoin which guarantees the security of the system but also leads to slow read and write speed [6]. Emercoin and Bitforest face the same problem of low throughput. ENS is mounted on Ethereum, when the transaction is intensive, it will cause a lack of computing resources and then reduce the availability and usability of the system [7].

However, the systems mentioned above split the domain namespace and only support the resolution of specific top-level domains. Also, the resolution of specific top-level domain names requires new plug-ins or tools, and the split domain namespace reduces the universality and usability. Some scholars have also proposed solutions compatible with the DNS. Wang et al. [8] proposed Blockzone, which uses an improved Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to provide domain name resolution service. Liu et al. [9] proposed FI-DNS which replaces the single root with root alliance and completed storage of the domain name below the root by blockchain, but the domain name resolution tree is forced transferring into two layers which decreases the efficiency. He et al. [10] proposed TD-Root which uses the consortium blockchain to construct a root zone management solution that ensures strong consistency and security of root zone data.

The above research results did not consider the decentralization of domain name publishing, also the resolution is running on a single-chain with low throughput. Polkadot [11] is a scalable multi-chain system. Polkadot provides a relay chain, on which there can be a large number of verifiable and globally dependent dynamic data structures, which we call para-chains. This feature can be used that we put domain name resolution on para-chains to improve flexibility and efficiency.

3 Domain Name Management Architecture Based on Relay Chain

First of all, a unified domain namespace is maintained in our architecture. The relay chain is used to interconnect between top level domains (TLD), providing cross-chain transaction means and ensuring the security of the blockchain. Para-chains provide second-level domain name management and resolution services. Finally, trusted off-chain storage of domain names is designed. Para-chains could improve the capability of domain name services. Both the relay chain and the para-chain are deployed on the consortium blockchain.

3.1 Overall Architecture

The overall architecture designed in this paper is shown in Fig. 2. Compared with the traditional domain name system, the blockchain-based domain name system has the advantages of higher security and equality of all parties, especially for country code top-level domains.

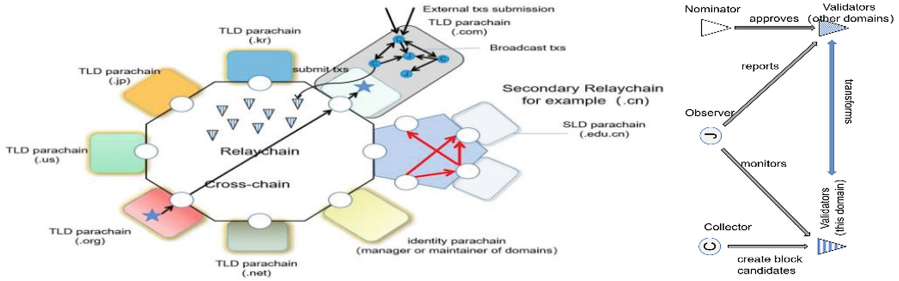

Fig. 2. Blockchain-based domain name management architecture diagram

The central relay chain maintains root domain zone files and para-chains maintain top-level domain zone files. Each para-chain that is directly connected to the relay chain manages a top-level domain ledger. The architecture supports multi-level access. The first-level para-chain can be used as the second-level relay chain. Four roles are involved, as shown in the right of Fig. 2. They are collectors, observers, nominators, and validators.

The collectors are groups that help validators create effective para-chain blocks. They are responsible for packaging new blocks and executing transactions (similar to miners). Then they submit a new block to one or more validators.

The observers are not directly related to the block packaging process. They exist at a supervisory level and punish validators who perform illegal actions. Observers can be rewarded as long as they report and prove that at least one secured party has illegal behaviors. Illegal actions include signing two different blocks with the same parent block, or approving an invalid block on a para-chain, or registering a malicious domain name.

The nominator is a group with rights and interests, and they entrust the security deposit to the validator. They invest in specific validators to maintain the blockchain.

The validators have the highest authority to help package new blocks. The validator needs to pledge enough deposit and must run a relay chain client on a highly available and high-bandwidth machine. On each block, the node must be prepared to receive a new block on the submitted para-chain.

3.2 Domain Name Storage Architecture

The storage architecture of the domain name is shown in Fig. 3. In the domain name storage architecture, we abstract the architecture into 3 layers. The blockchain layer defines different operation logics and stores all meta-transactions. Then, we separate the task of data location from the actual storage of data through the routing layer. We use zone files to store routing information. The storage layer is responsible for the actual storage of domain name data. All stored domain name data is signed by the key of the domain name owner. The off-chain storage method ensures that domain name owners can customize storage content without worrying about storage costs. We can verify the integrity of the data off-chain through the hash value stored in the control plane. The zone file of the domain name owner contains a URL record pointing to the domain name data. The data about to be written needs to be signed. Reading the data involves obtaining the zone file and the complete file. The public key is used to verify the signature of the data. So we deal with writing data at high speed due to the immutability of zone files in the blockchain.

3.3 Domain Name Management

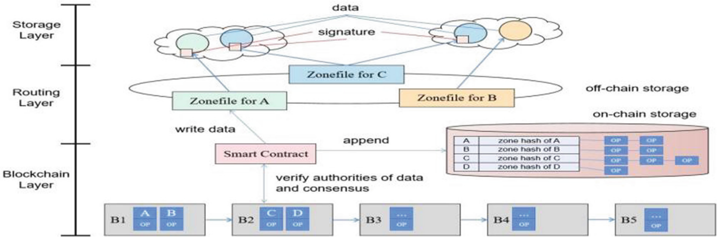

Fig. 3. Domain name storage architecture

Domain Name Registration. The process of domain name registration is shown in Fig. 4(a). Firstly, the domain name applicant as a user initiates a registration application to collectors and fills in the corresponding form (domain name, domain name ownership information, and domain name NS record). Collectors will process incoming requests in each slot, and then package them into candidate block and submit them to the validator. After the GRANDPA consensus, the validator will confirm the block and distribute the confirmed block to the collector. Then, the collector broadcasts it to all network. Finally, the blockchain returns the registration completed information to the user.

Domain Name Update. The process of domain name change is shown in Fig. 4(b). Similar to the domain name registration process, the type of transaction is domain name updating.

Domain Name Resolution. The policy process of domain name resolution is as follows. The user initiates a request to the resolver, and the resolver initiates a request to the corresponding para-chain. The required off-chain data is addressed through the smart contract and returned, and then returned to the user through the resolver.

4 Consensus Algorithm

The consensus algorithm is used to ensure the blockchain for producing blocks continuously and keeping data consistency of nodes. We use the mixed consensus of BABE and GRANDPA to ensure the stable operation of the blockchain. Hybrid consensus ensures that even if the network speed is fast, there will be no risk of delaying transactions, and there will be no stuck and rollback attacks.

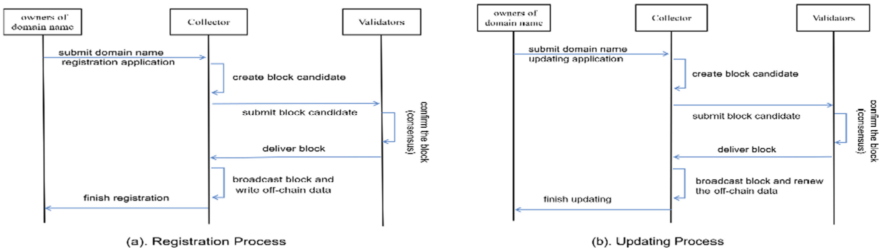
owners of domain name
Collector
Validators
submit domain name registration application
create block candidate
submit block candidate
confirm the block (consensus)
deliver block
broadcast block and write off-chain data
finish registration
(a). Registration Process
owners of domain name
Collector
Validators
submit domain name updating application
create block candidate
submit block candidate
confirm the block (consensus)
deliver block
broadcast block and renew the off-chain data
finish updating
(b). Updating Process

Fig. 4. Domain name management processes

Blind Assignment for Blockchain Extension (BABE). In each Slot, the validator uses the current slot number (Slot Number), the number of cycles (Epoch number), and the randomness of the chain (randomness) as the output to get a VRF output. If the obtained VRF is lower than a certain value, if it is, the validator gets a chance to produce a block. Each Slot generates a new block by the validator.

BABE divides the time into epochs. Each epoch is divided into several time intervals (slot). In each slot, some nodes that are eligible to produce blocks (slot leaders) are selected from a large number of nodes through VRF (verifiable random function). Here we call it a block producer. Each time interval (slot) selected block generation nodes may be different, there may be more than one, or none of them may be selected. Generally speaking, the probability of a node being selected is proportional to the number of tokens it pledges. As shown below:

The GHOST-Based Recursive Ancestor-Derived Prefix Protocol (GRANDPA). The GHOST-based recursive ancestor-derived prefix protocol provides near-instantaneous, asynchronous, and responsible security finality in the hybrid consensus blockchain (Fig. 5).

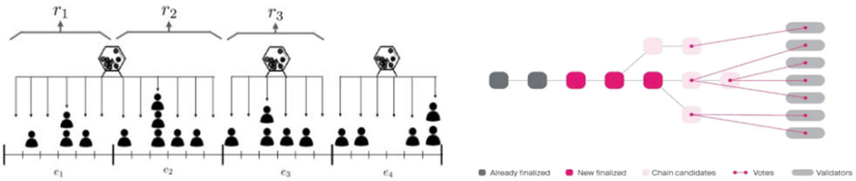

Fig. 5. BABE+GRANDPA

Hybrid consensus separates the finality decision from the block production mechanism. This is an efficient way to obtain the benefits of probabilistic finality and provable finality in our system. It also avoids the shortcomings: the possibility of unknowingly following false forks in probabilistic finality, and the problem of pausing in proving finality.

5 Conclusion

First of all, the architecture we proposed enables multiple parties involved in domain name maintenance to have equal management rights. The multiple parties involved in domain name maintenance could pledge assets to validators to maintain the top-level domain and realize the goal of co-governance by multi-parties.

Then, we use the relay chain structure and off-chain storage method. On the one hand, the management of domain names is assigned to different para-chains according to the top-level domains. On the other hand, the method of off-chain storage reduces the number of blockchain transactions. The combination of the two means improves the throughput of the blockchain.

Finally, due to the characteristics of the blockchain, the data hash stored on the blockchain could be used to verify the integrity of the data. Thereby the credible management of the domain name is ensured and domain name hijacking or domain name poisoning are avoided.

References

1. Mockapetris, P.V., Dunlap, K.J.: Development of the domain name system. Comput. Commun. Rev. **18**(4), 123–133 (1988)
2. Zhang, Y., Xia, C., Fang, B., Zhang, H.: An autonomous open root resolution architecture for domain name system in the internet. J. Inform. Secur. **2**(4), 57–69 (2017)
3. Gourley, S., Tewari, H.: Blockchain backed DNSSEC. In: Abramowicz, W., Paschke, A. (eds.) BIS 2018. LNBIP, vol. 339, pp. 173–184. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-04849-5_15
4. Hao Yang, E., Osterweil, D.M., Songwu, L., Zhang, L.: Deploying cryptography in Internet-scale systems: a case study on DNSSEC. IEEE Trans. Dependable Secure Comput. **8**(5), 656–669 (2011)
5. "Namecoin", http://namecoin.info
6. Ali, M., Nelson, J., Shea, R., Freedman, M.J.: Blockstack: A global naming and storage system secured by blockchains. In: 2016 {USENIX} annual technical conference ({USENIX}{ATC} 16), pp. 181–194 (2016)
7. Emercoin: Emercoin Links & Resources. https://emercoin.com/en/documentation/links-resources (2019)
8. Wang, W., Ning, H., Liu, X.: Blockzone: a blockchain-based DNS storage and retrieval scheme. In: Sun, X., Pan, Z., Bertino, E. (eds.) Artificial Intelligence and Security: 5th International Conference, ICAIS 2019, New York, NY, USA, July 26–28, 2019, Proceedings, Part IV, pp. 155–166. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-24268-8_15
9. Liu, W., Zhang, Y., Liu, L., Liu, S., Zhang, H., Fang, B.: A secure domain name resolution and management architecture based on blockchain. IEEE Symp. Comput. Commun. (ISCC) **2020**, 1–7 (2020). https://doi.org/10.1109/ISCC50000.2020.9219632
10. He, G., Su, W., Gao, S., Yue, J.: Td-root: a trustworthy decentralized dns root management architecture based on permissioned blockchain. Futur. Gener. Comput. Syst. **102**, 912–924 (2020)
11. "Polkadot Blockchain", https://polkadot.network/